

Analisis Peningkatan Keamanan Data *Two Step Verification* pada Aplikasi *Whatsapp Messenger*

M. Farid Abrar^{1*}, Muhammad Irwan Padli Nasution²

^{1&2} Fakultas Ekonomi dan Bisnis Islam, Prodi Manajemen,
Universitas Islam Negeri Sumatera Utara
Email : faridabrar14062004@gmail.com

Abstrak: Society era 5.0 merupakan kondisi dimana masyarakat dituntut untuk mengkaitkan setiap proses penyelesaian masalah melalui internet. Hal ini yang membuat teknologi semakin berkembang dan begitupula ide kejahatan yang memanfaatkan hal ini cyber spionage. Untuk itu whatsapp meningkatkan keamanan datanya dengan two step verification. Tujuan dilakukan penelitian ini adalah menambahkan kesadaran masyarakat dalam mengoperasikan elektronik khususnya whatsapp dengan fitur yang mereka keluarkan salah satunya two step verification yang memastikan bahwa pemilik akun masih memiliki akun aslinya.

Kata kunci: Era Sosial, Media Sosial, Keamanan Data

PENDAHULUAN

Seiring berjalannya waktu, teknologi semakin berkembang pesat dari waktu ke waktu. Hal ini yang membuktikan bahwa manusia memiliki pemikiran yang kritis dan berkembang. Kini kita berada pada era teknologi yang semakin canggih. 5.0 merupakan era resolusi dari revolusi 4.0. Society era 5.0 merupakan kondisi dimana masyarakat dituntut untuk menjadikan berbagai inovasi yang lahir pada era 4.0 sebagai penyelesaian berbagai tantangan dan masalah.

Era ini menjadi bentuk yang berarti semakin canggih nya teknologi maka tidak menutup kemungkinan semakin canggih pula cara dan teknik para oknum pelaku kejahatan akan mencuri data kita. Internet yang semakin canggih akan menjadi ancaman besar bagi manusia terutama pada keamanan data penggunaan. Maka dari ini, cyber espionage yakni kejahatan yang memanfaatkan kemajuan teknologi dan sistem informasi yang cukup maju seperti sekarang. Cyber spionage (Hamdan 2022) bisa merupakan bentuk upaya pengumpulan informasi bersifat umum ataupun khusus dalam sistem data pemerintah yang dijalankan oleh orang yang tidak berwenang dan memanfaatkannya. Hal ini dapat berupa bentuk mata – mata (spy) yang dilakukan mereka seperti layaknya spion.

Banyak pengguna yang masih enggan mencari tahu bagaimana data mereka dapat terjaga dari cybercrime. Hanya saja beberapa pengguna yang mendalami betapa pentingnya menjaga data dari kejahatan jenis digital ini. Kejahatan digital ini biasanya dapat berupa pesan, telfon, link, dan berbagai jenis bentuk kejahatan. Hal ini yang menjadikan whatsapp mengambil langkah sigap untuk mencegah pencurian data pribadi penggunanya.

Rahman dan Adnan (2017), menyebut facebook khawatir dengan 1,5 miliar penggunaanya akan terkena dampak hacking pada akun mereka, dengan demikian facebook menciptakan two step verification setiap penggunaanya ingin melakukan login namun bisa dicegah dengan beberapa jenis kejahatan seperti phishing, keylogger, peretasan ponsel, pencuri, dll.

TINJAUAN PUSTAKA

Keamanan data atau informasi yang merupakan bentuk menjaga kepribadian dalam bentuk data digital menggunakan alat elektronik yang bersifat rahasia dan sensitif dari akses yang tanpa sepengetahuan pemilik data. Prinsip utama pada keamanan data dan informasi adalah confidentiality(kerahasiaan), integrity(integritas) dan availability(ketersediaan) atau biasa sering disingkat CIA. Pada umumnya kerahasiaan akan dipengaruhi oleh integritas dan ketersediaan elektronik yang mampu menjaga kerahasiaan data.



Gambar 1. Model CIA

Dalam ilmu manajemen, ini menjadi pokok penting demi menjaga keamanan data dalam sebuah perusahaan yang mungkin saja nantinya akan diretas dan disalahgunakan oleh pihak yang tidak bertanggung jawab dengan mengatasnamakan perusahaan. Bukan hanya itu, data yang bocor juga akan mempengaruhi kualitas data yang nantinya akan berpengaruh pada master data management. Hal ini nantinya akan berpengaruh terhadap laba rugi dalam perusahaan. Perusahaan harus memastikan data yang didistribusi dan disimpan secara elektronik dapat tersalurkan dengan benar kepada user yang tepat. Sementara itu, kegagalan dalam sebuah perusahaan biasanya terjadi lebih besar akibat faktor internal karna kesalahan pengguna dalam melakukan pengoprasian sistem dibanding faktor external yang murni dilakukan oleh para hacker unggul.

Dalam masyarakat, sering terjadi pengoprasian sistem yang salah sebab tidak didasarkan pada keinginan untuk mencari cara mencegah data pribadi bercecer. Pemerintah yang seharusnya mampu mendalamkan dan memberikan arahan berbentuk iklan edukasi untuk meminimalisir resiko yang merugikan masyarakat.

Aplikasi whatsapp sendiri sebagai salah satu platform media sosial ternama memberikan judul dalam situs resminya yakni “dirancang untuk aman” dimana memberikan keterangan

bahwa whatsapp memberikan fitur inovatif yang nantinya akan mencegah pengguna untuk melakukan pengoprasian yang salah. Dalam keamanan whatsapp yang privasinya lebih terjamin dibanding media sosial lainnya sebab tidak ada satupun orang yang bisa mencari tahu nomor telepon pengguna kecuali dibagi, dikirim, dll. Whatsapp juga mendeteksi akun spam yang nantinya akan ditinjau oleh mereka. Bukan hanya itu, upaya yang mencurigakan diluar kendali kita akan diingatkan dan nantinya kita akan diberikan identifikasi verifikasi identitas untuk mencegah peretasan akun kita. Whatsapp menyediakan fitur speak up yakni melaporkan akun yang mengganggu, memberikan feedback, dll. Bukan hanya itu, fitur once seen juga merupakan keunggulan untuk menjadi privasi data yang dijalankan oleh whatsapp. Dan akhir-akhir ini whatsapp menampilkan fitur two step verification untuk meminimalisir masuknya akun dari perangkat lain.

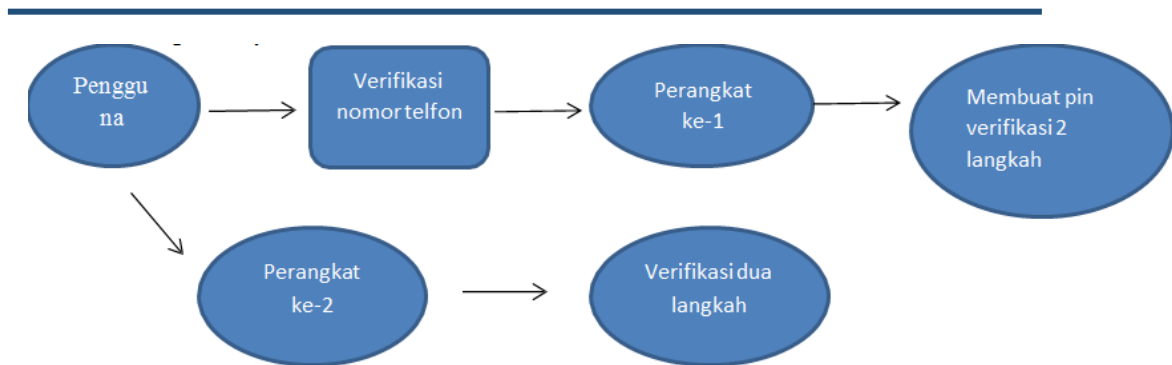
METODE PENELITIAN

Pada penelitian kali ini, peneliti akan menggunakan metode literature review dimana peneliti akan mengumpulkan pernyataan – pernyataan dari referensi yang terkait. Penelitian difokuskan kepada kesadaran masyarakat agar peneliti diharapkan mampu mengedukasi masyarakat luas demi mencegah terjadinya kebocoran data pribadi tanpa disengaja ataupun tersengaja karna wawasan yang hampir jarang.

HASIL DAN PEMBAHASAN

Two step verification atau verifikasi dua langkah yang diciptakan oleh whatsapp merupakan bentuk peningkatan keamanan data pribadi pengguna setelah bentuk keamanan sebelumnya seperti verifikasi nomor telfon, kunci aplikasi, enkripsi end to end, dll. Metode verifikasi dua langkah sendiri pada dasarnya digunakan untuk mencegah nomor telfon yang sudah kadaluwarsa dan didaur ulang oleh pihak provider dapat mengakibatkan login akun di dua handphone yang berbeda bagi yang mengaktivasi nomor daur ulang tersebut. Bukan hanya itu, hal ini akan menyulitkan kerja para hacker untuk melakukan peretasan akun whatsapp.

Two step verification berfungsi untuk memastikan bahwa pemilik aslinya masih memiliki akunnya. Menambahkan fitur ini juga memudahkan pengguna asli untuk berpindah perangkat dengan kepastian bahwa pengguna adalah satu satunya orang yang dapat mengaksesnya.



Gambar 2. Skema Two Step Verification

Dari skema diatas, dapat dilihat jika pengguna login ke perangkat baru akan diminta verifikasi 2 langkah yang telah dibuat pada login di perangkat 1

Hal ini tidak akan berguna jika penggunanya masih saja tidak mengaktifkan yang lain karena miss communication atau tidak tahu informasi bahwa ada nya fitur keamanan seperti ini. Untuk itu kesadaran ini penting khususnya kita sebagai generasi muda untuk terus membagi pemahaman khususnya kepada orang terdekat kita untuk mencegah hal yang tidak diinginkan terjadi. Banyak yang tidak menyadari banyak bentuk kegagalan keamanan yang mungkin akan menyerang kita tanpa kita sadari. Berikut contohnya :

1. Spam Chat

Ini merupakan bentuk kejahatan yang kemungkinan banyak pengguna belum tahu bentuk kejahatan seperti ini, kejahatan ini akan dimulai dengan modus “Assalamualaikum”, “selamat pagi”, dll yang merupakan bentuk sapaan dari pelaku kepada korban. Nantinya korban reflect membalas isi pesan tersebut dan alhasil pelaku mendapatkan informasi i.p adress pelaku melalui teknologi yang ia miliki untuk menyadap handphone korban. Pelaku akan memonitoring perangkat korban untuk mengetahui aktivitas korban saat membuka, log in akun, dll yang memungkinkan akan bermanfaat finansial bagi pelaku

2. Spam telfon

Sama seperti bentuk kejahatan pertama, jika anda mengangkat telfon dan melakukan instruksi sesuai yang dikatakan pelaku, maka handphone anda akan dengan mudah diretas.

3. Link Phising

Modus berikutnya adalah berbentuk link, ada berbagai macam bentuk penipuan pada modus ini salah satunya bentuk “jackpot, whatsapp memberi anda hadiah, anda memenangkan hadiah, klik untuk mendapatkannya” didalamnya, anda akan diminta untuk memasukkan nomor whatsapp dan verifikasi anda. Maka dari sini pelaku akan masuk ke akun anda.

4. Berpura pura menjadi teman

Ini adalah modus terpintar yang dilakukan oleh pelaku. Pada awalnya pelaku akan mencari informasi pribadi anda melalui media sosial lainnya tentang siapa teman dekat anda, keluarga anda, dll. Dan pelaku akan mulai berperan dengan mengatasnamakan nama kerabat anda. Dengan demikian langkah seperti pada modus pertama dapat dilancarkan dengan mudah oleh pelaku.

5. File

Ini merupakan modus yang marak dan mungkin sudah banyak yang tahu akan modus ini, namun tidak sedikit orang terjerat pada modus seperti ini. Pada awalnya pelaku akan mengirim bentuk aplikasi yang sudah ditanamkan virus kepada korban dengan memberikan nama yang nantinya akan membuat korban tertarik untuk mengklik dan menginstalnya seperti file undangan.

6. Button view

Merupakan modus yang sudah ada sejak 2022 kemarin, modus ini ialah bentuk file yang dikirim oleh pelaku dalam bentuk buram dan memberikan ikhtisar view dibawah file sehingga nantinya korban akan masuk dan dengan tidak sadar akan memasukkan kredensial akun penting yang nantinya pasti akan dihacking oleh pelaku.

Untuk mencegah hal diatas ialah :

1. Jangan memberikan kredensial username dan pin login sembarangan dan diusahakan jangan menyimpan hal ini di handphone anda, simpanlah dalam bentuk offline dengan menuliskannya pada buku catatan.
2. Matikan jaringan wifi dan bluetooth jika tidak digunakan mencegah terhubungnya konektivitas yang nantinya akan dimanfaatkan oleh pihak tak bertanggung jawab.
3. Memberikan jawaban pertanyaan keamanan untuk mengganti kata sandi lupa dengan jawaban palsu, mengapa? Karna biasanya pelaku akan dengan mudah memberikan jawaban jika anda memasukkannya dengan jawaban benar
4. Gunakan password dan pin yang tidak ada sangkutpaut yang menonjol pada diri anda, hal ini seringkali diabaikan pengguna dengan memasukkan pin sesuai dengan plat kendaraan, tanggal lahir, nomor rumah mereka.
5. Jangan gunakan password yang sama pada semua akun, ini untuk mencegah jika salah satu akun kebobolan, maka tidak semua akun ikut tertarik pada masalah ini.
6. Periksa permissions aplikasi, lisensi aplikasi sebelum menginstal.

KESIMPULAN

Fitur two step verification pada aplikasi Whatsapp sangat penting dalam menjaga kepemilikan akun hanya pada satu pengguna yang terlibat. Dengan demikian pada proses verifikasi login, pihak yang tidak bertanggung jawab akan lebih sulit untuk masuk karna harus mengetahui pin verifikasi yang telah dibuat pengguna sebelumnya. Untuk itu dengan adanya artikel ini, diharapkan masyarakat lebih berhati hati dan waspada dalam menjalankan sistem aplikasi salah satunya Whatsapp Messenger.

DAFTAR PUSTAKA

Khasanah, S., & Sutabri, T. (2023). ANALISIS PENCEGAHAN PENCURIAN DATA

MELALUI APLIKASI WHATSAPP MENGGUNAKAN METODE KRIPTOGRAFI. *Sainteks: Jurnal Sain dan Teknik*, 5(2), 145-153.

- Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis manajemen risiko keamanan data sistem informasi (Studi kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 2(1), 282-287.
- Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika: Media Hukum Dan Keadilan*, 25(01), 40-53.
- Pangaribuan, T., Sari, D., Takariani, C. S. D., & Simatupang, O. (2023). KESADARAN KEAMANAN DAN PRIVASI DATA PENGGUNA WHATSAPP (STUDI KASUS DI PROVINSI JAWA BARAT). *Jurnal Studi Komunikasi dan Media*, 27(1), 93-108.
- Rahman, M. M., & Adnan, M. A. (2017, January). Two step verification system of highly secure social media: Possible to breach the security. In *2017 International Conference on Networking, Systems and Security (NSysS)* (pp. 185-190). IEEE.
- Syafrizal, M. (2007, November). ISO 17799: Standar Sistem Manajemen Keamanan Informasi. In *Seminar Nasional Teknologi* (Vol. 2007, pp. 1-10).
- Yusnanto, T., Mustofa, K., Machmudi, M. A., & Wahyudiono, S. (2021). Tantangan Fenomena Keamanan Informasi Pasca Era Revolusi Industri 5.0. *TRANSFORMASI*, 17(2).