Renaldi Soeryadi, 72190301

1. Pelanggaran Data (*Data Breach*)

Pelanggaran Data merupakan salah satu ancaman umum yang mengincar data pengguna dengan mencuri data-data yang bersifat penting, termasuk data pribadi pengguna, dimana data tersebut nantinya dapat mengidentifikasi individu yang menggunakan layanan informasi tersebut, baik secara langsung maupun secara tidak langsung. Teknik *Data Breach* ini beragam, mulai dari Phising, Spear Phising, Injeksi kueri SQL, penipuan dukungan teknis (*Tech Support Scam*), dan lain-lain.

Salah satu contoh dari Data Breach ini adalah kasus dugaan adanya ratusan halaman *phising* dalam *game* PUBG Mobile, dimana Kaspersky, salah satu penyedia layanan keamanan data, menemukan ratusan halaman *phising* yang menargetkan pemain dengan mengirimkan hadiah bodong dengan mengirimkan akun *game ID* mereka melalui profil Twitter atau *Facebook*, dimana Ketika entri untuk mendapatkan hadiah gagal, mereka akan meminta informasi tambahan, seperti nama alias yang dipakai dalam *game*, nomor telepon, dan informasi detail pemain, sehingga para penipu (*scammer*) bukan hanya memiliki akun media sosial pengguna dari entri pertama, tetapi juga detail informasi pemain yang diletakkan dalam game sehingga akun game tersebut dapat dieproleh dan bahkan dapat dijual untuk mendapatkan keuntungan (Wardani, 2020).

Salah satu contoh berikutnya adalah dengan Penipuan Dukungan Teknis (*Tech Support Scam*), dimana para penipu menggunakan berbagai cara agar pengguna menanggap bahwa *platform* yang digunakan itu adalah asli atau/dan dapat dipercaya, seperti menggunakan situs web yang dapat dipercaya orang atau menggunakan layanan *call center*. Setelah korban menghubungi para penipu melalui layanan *call center,* para penipu meminta pengguna untuk mengunduh suatu program yang dianggap dapat men-diagnosa masalah yang dihadapi, tetapi setelah terhubung melalui aplikasi tersebut, penipu dapat mengakses dan mencuri seluruh data pribadi pengguna, seperti data perbankan, data rekam medis, dan data pribadi yang dapat diakses, dan datanya dapat dijual untuk kepentingan pribadi, bahkan menngambil dana yang sudah dibayarkan oleh para korban dengan total yang terbilang besar (CBC News, 2019).

1. Serangan Kamus (*Dictionary Attack*)

Serangan kamus merupakan suatu serangan yang dapat mencuri data pengguna dengan mencoba menggunakan kata sandi yang sudah diketahui, seperti tanggal lahir dan kata sandi umum. Serangan kamus ini biasa disebut dengan *Brute Force Attack*, karena memiliki Teknik yang serupa. Serangan Kamus ini berbahaya bagi pengguna, karena dapat menyebabkan data pengguna bocor dan memungkinkan data anda dicuri, dijual, atau digunakan untuk merusak reputasi korban dengan melancarkan perusakan website atau menyebarkan konten *hoax* atau illegal menggunakan akun anda (Golden Fast Network, 2020).

Salah satu contoh dari Serangan Kamus adalah Bocornya 500 juta data LinkedIn dalam forum online *hacker*, dimana pelaku berhasil masuk kedalam sistem dan mengekstrasi setidaknya 500 juta profil LinkedIn, yang dijual dengan harga setidaknya 4 digit, namun seseorang berhasil membeli contoh datanya debgan harga sekitar 2 dollar AS. Dalam 500 juta data yang berhasil bocor tersebut, terdapat data-data sensitive penggunanya, seperti nama lengkap, alamat surat elektronik (e-mail), nomor telepon, gender pengguna, tautan profil media sosial, informasi pekerjaan, dan lain-lain (Pertiwi, 2021).

1. Ransomware

Ransomware adalah serangan yang disebabkan oleh malware, sebuah aplikasi yang memiliki kode-kode yang memyebabkan kerusakan dan menggangu perangkat normal dengan memberikan akses tidak sah kepada penyerang dan mencuri serta membuat anda tidak dapat mengakses data-data yang digunakan dengan mengenkripsi data-data yang dicuri dan memeras korbannya untuk meminta imbalan, biasanya dengan menggunakan mata uang kripto (*Cryptocurrency*) dengan imbalan kunci dekripsi yang dapat digunakan untuk membuka Kembali akses datanya.

Salah satu contoh kasus Ransomware yang terkenal di Indonesia adalah serangan WannaCrypt atau serangan WannaCry pada tahun 2017, yang membuat dua rumah sakit di Jakarta menjadi korbannya, yaitu RS. Harapan Kita dan RS. Dharmais. Para penyerang menggunakan *malicious software*, yaitu sebuah software yang dapat menyerang computer korban. Akibatnya, hampir seluruh sistem TI rumah sakit pun terkena dampaknya, karena data-data rumah sakit pun dikunci sehingga seluruh data pasien dan data pembayaran rumah sakit pun tidak dapat diakses (Kertopati, 13).

1. Serangan Yang Menggangu (*Disruptive Attacks*)

Serangan Penolakan Layanan Terdistribusi (*Distributed Denial of Service (DDoS)*) atau yang biasanya disebut dengan Serangan Yang Menggangu (*Disruptive Attacks*) merupakan suatu serangan yang mencoba untuk melelahkan sumber daya aplikasi yang tersedia, sehingga membuat aplikasi tersebut tidak dapat diakses oleh penggunanya, dengan menyasar titik temu (*endpoints*) yang mudah dijangkau poleh internet.

Salah satu kasus DDoS ini adalah serangan DDos terhadap situs Wikipedia dengan menyasar server utamanya, yatu Server Wikimedia. Hal itu membuat situs Wikipedia lumpuh (*Offline*) di 5 negara di Eropa, yaitu di Inggris, Polandia, Perancis, Jerman, dan Italia, pada 7 september 2019. Hal ini bukan hanya melumpuhkan situs Wikipedia saja, melainkan juga seluruh layanan serupa yang didirikan oleh Wikimedia Foundation, seperti Wikiquote, Wikibooks, Wikisource, Wikispecies, dan Wikiversity (Tim CNN Indonesia, 2019).

1. Coal Miners (Penambang Koin)

Penambang Koin merupakan serangan yang menargetkan mata uang kripto (*Cryptocurrency*) yang ada dalam sistem yang dibobol, dengan mengakses secara illegal kedalam sistem dan mencuri mata uang kripto yang ada didalamnya.

Salah satu contoh Penambang Koin ini adalah pembobolan Uang Kripto di Jepang, yang membuat uang sebesar 1,4 triliun rupiah lenyap. Hal ini bermula ketika Liquid, perusahaan yang melayani transaksi mata uang kripto asal Jepang, mendeteksi adanya akses illegal pada beberapa sistem mereka, yang kemudian Bersama dengan dengan perusahaan yang bertugas melacak pergerakan mata uang yang berbasis di London, Elliptic, menemukan uang sebesar 97 juta Dolar Amerika Serikat diterima oleh seseorang yang diidentifikasi sebagai pencuri (Kompas.com, 2021).

Daftar Pustaka

CBC News. (2019, Oktober 5). *Busting tech support scammers: Undercover in India (Marketplace).* Retrieved from https://www.youtube.com/watch?v=NGiznJMGM-0

Golden Fast Network. (2020, November 20). *Brute Force Attack: Pengertian, Tipe & Langkah Mencegahnya*. Retrieved from Golden Fast Network: https://www.goldenfast.net/blog/brute-force-adalah/

Kertopati, L. (13, Mei 2017). *Dua Rumah Sakit di Jakarta Kena Serangan Ransomware WannaCry*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/teknologi/20170513191519-192-214642/dua-rumah-sakit-di-jakarta-kena-serangan-ransomware-wannacry

Kompas.com. (2021, Agustus 22). *Terjadi Pencurian Uang Kripto Lagi, Rp 1,4 Triliun Digondol Hacker di Jepang*. Retrieved from Kompas.com: https://www.kompas.com/global/read/2021/08/22/091849870/terjadi-pencurian-uang-kripto-lagi-rp-14-triliun-digondol-hacker-di

Pertiwi, W. K. (2021, April 10). *Data 500 Juta Pengguna LinkedIn Bocor, Dijual Mulai Rp 30.000*. Retrieved from Kompas.com: https://tekno.kompas.com/read/2021/04/10/07020017/data-500-juta-pengguna-linkedin-bocor-dijual-mulai-rp-30000

Tim CNN Indonesia. (2019, September 9). *Diserang DDoS, Wikipedia Lumpuh di Beberapa Negara Eropa*. Retrieved from CNN Indonesia: https://www.cnnindonesia.com/teknologi/20190909124531-185-428718/diserang-ddos-wikipedia-lumpuh-di-beberapa-negara-eropa

Wardani, A. S. (2020, November 25). *PUBG Mobile Diburu Ratusan Serangan Phishing yang Ingin Curi Akun Pengguna*. Retrieved from Liputan 6: https://www.liputan6.com/tekno/read/4417298/pubg-mobile-diburu-ratusan-serangan-phishing-yang-ingin-curi-akun-pengguna