JURNAL HUKUM, POLITIK DAN ILMU SOSIAL (JHPIS)
Vol.3, No.3 September 2024
e-ISSN: 2963-7651; p-ISSN: 2963-8704, Hal 155-161
DOI: https://doi.org/10.55606/jhpis.v3i2.3900

Mengoptimalkan Implementasi UU No. 27 Tahun 2022 Dengan Penetration Test Dan Vulnerability Assessment Pada Kasus Pembobolan Data Aplikasi Dana

Tabitha Fransisca Romauli Nababan, Shevanna Putri Cantiqa
Universitas Pembangunan Nasional "Veteran" Jakarta

Alamat: Jalan RS. Fatmawati Raya, Pondok Labu, Cilandak, South Jakarta City, Jakarta 12450
Korespodensi email : 2210611214@mahasiswa.upnvj.ac.id

Abstract. *Data security in digital financial applications such as mobile banking, e-wallets, and online payment services is very important. However, there are many security risks lurking. Irresponsible parties can exploit security gaps to steal personal information. The ITE Law regulates the limitations, obligations, and responsibilities of parties involved in electronic systems, including service providers, data managers, and users as well as sanctions for cybercriminals. One of the main weaknesses in a financial application is the lack of strict and consistent security standards. Due to the many acts of cybercrime, it is important for companies to take preventive measures, one of which is through Vulnerability Assessment and Penetration Testing (VAPT). VAPT can help identify and fix vulnerabilities in applications before they are exploited by cybercriminals.*
Keywords: *data security, security vulnerabilities , e-wallet,*

Abstrak. Keamanan data dalam aplikasi finansial digital seperti mobile banking, e-wallet, dan layanan pembayaran online sangatlah penting. Namun, terdapat banyak risiko keamanan yang mengintai. Pihak tidak bertanggung jawab dapat memanfaatkan celah keamanan untuk mencuri informasi pribadi tersebut. UU ITE mengatur batasan, kewajiban, dan tanggung jawab para pihak yang terlibat dalam sistem elektronik, termasuk penyedia layanan, pengelola data, dan pengguna serta sanksi bagi pelaku kejahatan siber. Salah satu kelemahan utama dalam sebuah aplikasi finansial adalah kurangnya standar keamanan yang ketat dan konsisten. Oleh karena banyaknya tindak kejahatan dunia maya, penting bagi perusahaan untuk mengambil langkah pencegahan, salah satunya dengan Vulnerability Assessment dan Penetration Testing (VAPT). VAPT dapat membantu mengidentifikasi dan memperbaiki kerentanan dalam aplikasi sebelum dieksploitasi oleh penjahat cyber.
Kata Kunci: keamanan data, kerentanan keamanan, dompet digital.

LATAR BELAKANG

Perkembangan teknologi informasi, terutama internet, memberikan dampak besar pada berbagai aspek kehidupan manusia. Berdasarkan laporan We Are Social, pada Januari 2024, terdapat 185 juta pengguna internet di Indonesia, yang setara dengan 66,5% dari total populasi nasional yang mencapai 278,7 juta orang. Dengan berkembangnya internet, teknologi informasi semakin mempengaruhi cara orang berkomunikasi, bekerja, dan berinteraksi dengan dunia luar. Meskipun teknologi informasi memiliki banyak manfaat dan kemudahan, terdapat juga risiko, terutama terkait keamanan data.

Keamanan data sangat penting untuk aplikasi finansial seperti mobile banking, e-wallet, dan layanan pembayaran digital, karena aplikasi ini menyimpan informasi pribadi seperti nomor rekening, saldo, detail kartu kredit/debit, dan riwayat transaksi. Diantara 15 negara lainnya, Indonesia menempati peringkat ketiga dalam *Laporan State of Finance App Marketing* edisi 2021, yang dirilis oleh *AppsFlyer*. Hal ini menunjukkan bahwa orang

Received Mei 07, 2024; Accepted Juni 19, 2024; Published September 30, 2024
*Tabitha Fransisca Romauli Nababan, 2210611214@mahasiswa.upnvj.ac.id

Indonesia sangat bergantung pada aplikasi keuangan untuk memenuhi berbagai kebutuhan keuangan mereka.

Dibalik kemudahan yang ditawarkan oleh aplikasi finansial juga terdapat banyak resiko yang terjadi. Pihak yang tidak bertanggung jawab dapat memanfaatkan celah keamanan untuk mengumpulkan informasi pribadi seperti nomor rekening, saldo, informasi kartu kredit dan debit, serta rekaman transaksi. Hal ini jelas merupakan pelanggaran privasi yang dapat membahayakan pengguna tersebut.

Maraknya kasus pembobolan data yang terjadi pada aplikasi finansial menunjukkan bahwa semakin banyak aktivitas dan data yang dikelola secara digital, semakin besar kemungkinan terjadinya pelanggaran keamanan data. Kasus pembobolan data pada aplikasi Dana adalah contoh dari kelemahan keamanan yang perlu diperbaiki, yang menunjukkan betapa pentingnya mengambil tindakan proaktif untuk meningkatkan Pelindungan data dan mencegah kejadian serupa terjadi di masa depan.

Kasus ini bermula dari kisah viral di media sosial mengenai seorang pengguna yang kehilangan dana besar dalam akun DANA miliknya. Pada Januari lalu, medio pekan ini beredar cerita viral ihwal seseorang kehilangan uang sebesar Rp6 juta di salah satu platform dompet digital, DANA, milik PT Espay Debit Indonesia Koe. Salah satu akun bernama @tarorumput di media sosial menceritakan saldo tabungannya raib hingga hanya tersisa Rp 836. Hilangnya saldo tersebut dia sadari setelah mengetahui ada transaksi mencurigakan melalui *QRIS* dari akunnya.

Oleh karena itu, perlu adanya penerapan *Vulnerability Assessment* dan *Penetration Testing* untuk mengatasi kasus ini, sehingga implementasi Undang Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi. Berdasarkan uraian diatas maka menjadi penting untuk dilakukan penelitian yang dituangkan pada judul **"**Mengoptimalkan Implementasi UU No. 27 Tahun 2022 Dengan *Penetration Test* Dan *Vulnerability Assessment* Pada Kasus Pembobolan Data Aplikasi Dana".

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan undang-undang. Data yang dibutuhkan peneliti termasuk informasi tentang peraturan yang mengatur data pribadi dan statistik tentang tindak kejahatan yang memanfaatkan data pribadi. Data yang dianalisis bersumber dari data sekunder, mencakup sumber hukum primer dan sekunder. Sumber hukum primer melibatkan UUD 1945 dan UU Nomor 27 Tahun 2022 tentang

Pelindungan Data Pribadi. Sementara itu, bahan hukum sekunder mencakup jurnal ilmiah, buku, dan dokumen hukum terkait lainnya.

Pendekatan yang digunakan dalam penelitian kali ini adalah *statue approach* yang sebagai landasan utama penelitian ini. Pendekatan penelitian ini adalah penelitian kepustakaan, yang mengindikasikan bahwa penulis membaca, memahami, dan menyimpulkan dari peraturan perundang-undangan, buku, jurnal, berita, dan artikel yang relevan dengan topik.

HASIL DAN PEMBAHASAN

Kelemahan Utama Dalam Implementasi UU No. 27 Tahun 2022 Terhadap Pembobolan Data dalam Aplikasi Dana.

Kekhawatiran masyarakat mengenai keamanan data pribadi dan transaksi digital semakin meningkat setelah adanya kasus pembobolan data yang terjadi pada aplikasi DANA. Insiden ini telah menyebabkan banyak pengguna kehilangan dana dalam jumlah yang cukup besar karena upaya peretasan dan pencurian data oleh pihak-pihak yang tidak bertanggung jawab. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Informasi dan Transaksi Elektronik (UU ITE) telah diundangkan sebagai payung hukum untuk mengatur keamanan informasi dan transaksi elektronik, namun kejadian pembobolan data di DANA mengindikasikan adanya kelemahan dalam implementasi UU ITE tersebut.

Perlindungan data pribadi seharusnya menjadi tanggung jawab pemerintah, karena data pribadi merupakan bagian dari hak asasi setiap warga negara (Priliasari, 2023). Kehadiran UU ITE merupakan upaya pemerintah untuk menjamin keamanan dan melindungi kepentingan serta hak-hak pengguna layanan elektronik, khususnya terkait Perlindungan data pribadi dan informasi pribadi. UU ITE mengatur batasan, kewajiban, dan tanggung jawab para pihak yang terlibat dalam penyelenggaraan sistem elektronik, seperti penyedia layanan, pengelola data, dan pengguna akhir. Selain itu, UU ITE mengatur tindak pidana yang berkaitan dengan pelanggaran keamanan informasi dan transaksi elektronik, serta sanksi yang dapat dijatuhkan kepada pelaku kejahatan siber.

Ketiadaan standar keamanan yang ketat dan konsisten untuk seluruh penyedia layanan aplikasi keuangan digital merupakan salah satu kelemahan utama yang ditemukan dalam kasus ini. Hal ini memungkinkan pihak-pihak yang tidak bertanggung jawab untuk melakukan serangan siber dan mencuri data pribadi dengan memanfaatkan kelemahan keamanan pada aplikasi tertentu. Setiap penyedia aplikasi keuangan digital seharusnya memiliki kewajiban untuk menerapkan standar keamanan yang tinggi secara konsisten untuk

melindungi data pengguna. Namun, jika tidak ada pedoman atau peraturan yang jelas mengenai standar keamanan minimum yang harus dipenuhi, kemungkinan besar penyedia layanan akan berbeda dalam hal keamanan.

Faktor lain yang berperan adalah kurangnya edukasi dan kesadaran masyarakat mengenai pentingnya keamanan data serta praktik terbaik dalam melindungi informasi pribadi. Akibatnya, pengguna aplikasi keuangan digital lebih rentan terhadap serangan phishing dan berbagai bentuk penipuan lainnya yang dapat menyebabkan data mereka bocor. Pengguna berpotensi menjadi korban pembobolan data dan penggunaan data pribadi untuk tujuan ilegal jika mereka tidak tahu bagaimana melindungi data pribadi mereka secara aman atau tidak waspada terhadap cara pelaku kejahatan siber bertindak.

Sebagai pengguna sistem elektronik, terdapat kewajiban untuk menjaga kerahasiaan data pribadi yang diperoleh, dikumpulkan, diolah, dan dianalisis. Data pribadi tersebut hanya dapat digunakan sesuai dengan keperluan pengguna semata. Pengguna juga bertanggung jawab untuk menjaga data pribadi beserta dokumen yang memuat informasi tersebut dari penyalahgunaan. Tanggung jawab ini berlaku baik dalam lingkup organisasi yang menjadi kewenangannya maupun dalam kapasitas individu, apabila terjadi tindakan penyalahgunaan terhadap data pribadi yang berada dalam penguasaannya (Benuf Dkk., 2019).

Dalam kasus aplikasi DANA, perlu dilakukan pemeriksaan lebih lanjut terhadap kelemahan sistem keamanan yang ada serta prosedur yang telah digunakan untuk melindungi data pengguna baik sebelum maupun setelah pembobolan. Pihak DANA harus menemukan kelemahan atau celah keamanan apa pun dalam sistem aplikasi DANA yang memungkinkan pembobolan data oleh pihak tidak bertanggung jawab.

Penerapan *Vulnerability Assessment* dan *Penetration Testing* dapat mengoptimalkan implementasi UU No. 27 Tahun 2022.

Perkembangan teknologi informasi dan komunikasi membawa kemudahan bagi kehidupan manusia saat ini. Salah satu hal yang berkembang pesat adalah aplikasi web. Aplikasi berbasis web dipilih karena aplikasi tersebut merupakan sebuah platform dengan fitur dan kegunaan yang tersedia mudah digunakan. Kemudahan-kemudahan yang diberikan oleh aplikasi inilah yang juga menjadi alasan mengapa banyak masyarakat merasa nyaman untuk menggunakannya dan sangat terbantu untuk menghemat waktu (Yudha Dkk., 2018).

Banyaknya aplikasi yang tersedia menjadi tantangan tersendiri untuk perusahaan pengembang aplikasi dalam memperkuat keamanan pada aplikasi mereka tersebut.Tidak dapat dipungkiri, seiring dengan perkembangan zaman, teknologi juga ikut berkembang.

Dampak yang ditimbulkan dari perkembangan tersebut tidak hanya positif tetapi juga negatif. Kemudahan dan hemat waktu merupakan salah satu dampak positif yang diberikan oleh aplikasi web, sementara kebocoran data atau kehilangan uang merupakan dampak negatif yang dihasilkan dari aplikasi web tersebut (Budiman Dkk., 2021).

Seperti halnya pada aplikasi DANA. Aplikasi ini merupakan layanan penyedia sistem pembayaran atau dompet digital yang dapat digunakan untuk pembayaran, tabungan, ataupun transfer dana dari satu pengguna ke pengguna lain. Tidak hanya sesama aplikasi, DANA dapat melakukan transfer ke berbagai aplikasi ataupun rekening bank. DANA berbasis mobile sehingga mengharuskan penggunanya untuk download aplikasi terlebih dahulu dan melakukan pendaftaran data diri melalui perangkat telekomunikasi.

Pendaftaran data diri merupakan hal yang wajib dilakukan ketika melakukan registrasi akun pada aplikasi dompet digital sebagai syarat keamanan akun yang meliputi nama lengkap, nomor telepon, alamat email aktif, dan kata sandi untuk mengamankan akun. Kemudian, data nasabah yang telah terkumpul akan terkirim kepada pusat pengelola keamanan aplikasi yang akan dilindungi dari kemungkinan-kemungkinan buruk dalam bertransaksi. Namun saat ini, masih banyak kasus-kasus kebocoran data pribadi nasabah seperti yang terjadi pada aplikasi DANA dompet digital. Bukan hanya data pribadi saja, tetapi saldo yang ada di dalam DANA hilang. Diduga hal tersebut terjadi karena kode verifikasi pemilik akun DANA tersebar secara tidak sengaja melalui phising ataupun cara-cara lain yang membocorkan informasi penting terkait akun pribadi customer kepada hacker.

Tentu saja hal-hal tersebut akan membawa dampak untuk keberlangsungan bisnis perusahaan. Contohnya, jika aplikasi terkena hack, otomatis minat customer akan berkurang karena menganggap aplikasi tersebut tidak aman. Di lain sisi, hal tersebut juga menyebabkan kerugian materil untuk korban. Meskipun perusahaan tersebut ada dibawah naungan pengawasan negara, namun kepercayaan customer/trust dan reputasi perusahaan tetap akan berkurang. Disinilah kita dapat menilai betapa pentingnya perlindungan konsumen guna kelangsungan operasional aplikasi berbasis web (Threats, 2021).

Untuk mencegah terjadinya kejadian serupa, maka penting bagi perusahaan untuk mengambil langkah pencegahan terlebih dahulu. Dalam hal inilah *Vulnerability Assessment* dan *Penetration Test* dapat menjadi sebuah solusi positif guna mencegah kesalahan-kesalahan dalam berjalannya sebuah aplikasi. *Vulnerability Test* wujudnya adalah laporan yang mencakup konfigurasi dan kerentanan pada sebuah situs. Data yang diperoleh dari *Vulnerability Assessment (VAPT)* akan diteliti kembali dan setelahnya dicari celah keamanan

yang mungkin terjadi yang selanjutnya diberikan solusi. Atau, perbaikan celah keamanan yang ada dengan semaksimal mungkin untuk meningkatkan keamanan website.

Undang-Undang PDP mewajibkan perusahaan untuk mengambil tindakan keamanan serius untuk melindungi data pribadi dari akses, pengungkapan, penggunaan, perubahan, atau penghancuran yang tidak sah. VAPT dapat membantu organisasi mengidentifikasi dan menerapkan langkah-langkah keamanan yang diperlukan. VAPT juga berperan dalam mengidentifikasi kerentanan dan kelemahan sistem informasi yang bisa disalahgunakan untuk mencuri, mengubah, atau menghapus informasi pribadi. Penting untuk mengikuti prinsip-prinsip dasar UU PDP, seperti akuntabilitas, batasan sasaran, dan minimalisasi data.

VAPT bisa digunakan sebagai alat untuk mengidentifikasi celah keamanan pada sistem informasi untuk tindak kejahatan phising. Pelaku kejahatan sering kali menggunakan teknik phising untuk mendapatkan data pribadi. Dengan mengidentifikasi celah ini, perusahaan dapat mengambil langkah untuk memperbaikinya dan memperkuat perlindungan dari serangan phishing. VAPT juga dapat menolong perusahaan untuk memastikan bahwa kontrol akses mereka efektif dan hanya pihak berwenang saja yang bisa mengakses data pribadi.

Sedangkan penetration test Hanya memberikan gambaran singkat tentang sistem keamanan informasi yang diterapkan, seperti apakah pengamanan pada aplikasi tersebut sudah efektif atau tidak. Hal ini hanya dapat dilakukan dengan cara *penetration test*. Berdasarkan hal tersebut, penilaian kerentanan dapat memberikan nilai lebih bagi suatu perusahaan dibandingkan dengan hanya sebatas penjagaan saja. pengujian penetrasi, mengkaji pentingnya sistem pengendalian yang efektif (Fathurahman, 2022).

Baik *Penetration test* ataupun *Vulnerability assessment*, keduanya merupakan tindakan preventif untuk menguji kekuatan keamanan data pada aplikasi yang sesuai dengan perwujudan keamanan customer pada Undang-Undang Nomor 27 tahun 2022. Saat ini, sudah banyak badan-badan swasta yang menyediakan layanan untuk perusahaan yang ingin melakukan tes keamanan pada aplikasi yang mereka miliki, contohnya seperti *Fourtrezz* dan *Threats.*

KESIMPULAN

Dibalik kemudahan yang ditawarkan oleh aplikasi finansial juga terdapat banyak resiko yang terjadi. Pihak yang tidak bertanggung jawab dapat memanfaatkan celah keamanan untuk mengumpulkan informasi pribadi seperti nomor rekening, saldo, informasi kartu kredit dan debit, serta rekaman transaksi. Maraknya kasus pembobolan data yang terjadi pada aplikasi

finansial menunjukkan bahwa semakin banyak aktivitas dan data yang dikelola secara digital, semakin besar kemungkinan terjadinya pelanggaran keamanan data. UU ITE mengatur batasan, kewajiban, dan tanggung jawab para pihak yang terlibat dalam penyelenggaraan sistem elektronik, seperti penyedia layanan, pengelola data, dan pengguna akhir. Selain itu, UU ITE mengatur tindak pidana yang berkaitan dengan pelanggaran keamanan informasi dan transaksi elektronik, serta sanksi yang dapat dijatuhkan kepada pelaku kejahatan siber. Untuk mencegah terjadinya kejadian serupa, maka penting bagi perusahaan untuk mengambil langkah pencegahan terlebih dahulu. Dalam hal inilah *Vulnerability Assessment* dan *Penetration Test* dapat menjadi sebuah solusi positif guna mencegah kesalahan-kesalahan dalam berjalannya sebuah aplikasi.

DAFTAR PUSTAKA

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Pelindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia: Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, *3*(2), 145-160.

Budiman, A., Ahdan, S., & Aziz, M. (2021). Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assessment. Jurnal Komputasi, 9(2).

Databoks, (2024), 'Ada 185 Juta Pengguna Internet Di Indonesia Pada Januari 2024', Https://Databoks.Katadata.Co.Id/Datapublish/2024/02/27/Ada-185-Juta-Pengguna-Internet-Di-Indonesia-Pada-Januari-2024, Diakses Pada Tanggal 1 Juni 2024.

Duwitmu.Com. 2022. "Apa Itu Dana Dompet Digital E-Wallet: Cara Daftar, Aktivasi". Https://Duwitmu.Com/Tabungan/Dana-Dompet-Elektronik. Diakses Pada 1 Juni 2024

F. Yudha, A. Muhammad, And P. Muryadi. (2018) "Perancangan Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis Web," *Cyber Security Dan Forensik Digit., Vol. 1, No. 1, Pp. 1–6.*

Fathurahman, M., & Aziz, A. (2022). Vulnerability Assessment Dan Penetration Test Pada Website Ma/Mts Husnul Khatimah Kuningan. In Prosiding Seminar Nasional Terapan Riset Inovatif (Sentrinov) (Vol. 8, No. 3, Pp. 138-145).

Katadata, (2022), 'Indonesia Pengguna Fintech Tertinggi Ketiga Di Dunia', Https://Katadata.Co.Id/Digital/Fintech/60d1c95ea19bb/Indonesia-Pengguna-Fintech-Tertinggi-Ketiga-Di-Dunia, Diakses Pada Tanggal 5 Juni 2024.

Priliasari, E. (2023). Pelindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional*, *12*(2).

Threats, C. C. (2022). Cyber Security Culture.