Pusat Analisis Keparlemenan
Badan Keahlian DPR RI
Gd. Nusantara I Lt. 2
Jl. Jend. Gatot Subroto
Jakarta Pusat - 10270
☎ 5715409 🖷 5715245
✉ infosingkat@gmail.com

BIDANG POLITIK, HUKUM, DAN KEAMANAN

INFO Singkat

KAJIAN SINGKAT TERHADAP ISU AKTUAL DAN STRATEGIS

Vol. XVI, No. 13/I/Pusaka/Juli/2024

6

LEMAHNYA PENGAMANAN PUSAT DATA NASIONAL SEMENTARA TERHADAP SERANGAN SIBER

Aryojati Ardipandanto*

Abstrak

Pusat Data Nasional Sementara (PDNS) di Surabaya mendapatkan serangan siber pada 20 Juni 2024 oleh Grup Hacker Lockbit. Serangan siber itu berdampak pada terganggunya layanan keimigrasian serta tercurinya data-data milik Badan Intelijen Strategis TNI dan POLRI. Data curian tersebut telah dijual di "dark web". Tulisan ini mengkaji faktor penyebab lemahnya pengamanan PDNS terhadap serangan siber. Kelemahan yang masih ada yaitu pertama, sistem pengamanan yang diimplementasikan hanya menggunakan Windows Defender sehingga sangat rentan diserang hacker. Kedua, anggaran negara untuk menanggulangi serangan siber belum memadai. Ketiga, belum ada perintah tegas dalam peraturan perundang-undangan yang mewajibkan instansi pemerintah segera memutakhirkan sistem pengamanan sibernya. Pada fungsi legislasi, Komisi I DPR RI dan pemerintah harus segera membuat UU tentang Satu Data Indonesia dengan peraturan terkait pengamanan siber. Pada fungsi pengawasan, Komisi I DPR RI perlu meningkatkan pengawasannya atas kinerja Kemenkominfo RI dan BSSN dalam menyediakan pengamanan siber bagi PDNS secara berkesinambungan.

Pendahuluan

Pada 20 Juni 2024 terjadi serangan siber terhadap sistem Pusat Data Nasional Sementara (PDNS) di Surabaya. Serangan siber tersebut disebabkan serangan perangkat keras perusak atau *ransomware Brain Chipper*. Menteri Komunikasi dan Informatika Republik Indonesia (Menkominfo RI) Budi Arie Setiadi menyampaikan bahwa yang diserang adalah PDNS 2 di Surabaya. Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo RI) masih berfokus pada pemulihan akibat serangan dengan bantuan Badan Siber dan Sandi Negara (BSSN). *Hacker* melakukan penyerangan

* Analis legislatif Ahli Muda Bidang Politik, Hukum, dan Keamanan Pusat Analisis Keparlemenan Badan Keahlian Setjen DPR RI, *email: aryojati.ardipandanto@dpr.go.id.*

PUSAKA BKD

9 772088 235001

dan meminta tebusan sebesar 8 juta dollar AS atau sekitar Rp131,6 milyar. Namun pemerintah tidak bersedia memenuhinya ("Keamanan Siber; Pemerintah Menolak Permintaan Peretas", 2024).

Hacker yang menyerang PDNS di Surabaya merupakan grup peretas yang menamakan diri sebagai Lockbit. Terakhir, grup ini mengeluarkan versi terbaru dari virusnya, yaitu Lockbit 3.0, yang disebut pula sebagai penyebab gangguan di Bank Syariah Indonesia ("Keamanan Siber; Pemerintah Menolak Permintaan Peretas", 2024). Ketua *Indonesia Cyber Security Forum* Ardi Sutedja mengatakan bahwa ini merupakan "bencana" siber berskala nasional ("Serangan Siber; Sepekan Insiden PDN Belum Bisa Dipulihkan", 2024).

Peristiwa penyerangan siber atas PDNS ini menunjukkan bahwa ternyata pengamanan atas data nasional pada PDNS belum bisa diandalkan. Oleh sebab itu, perlu dikaji apa saja faktor penyebab lemahnya pengamanan PDNS terhadap serangan siber. Tulisan ini membahas tentang kelemahan sistem pengamanan siber PDSN dan upaya yang perlu dilakukan pemerintah untuk mencegah dan mengatasi serangan siber agar tidak terulang kembali.

Kelemahan Sistem Pengamanan Siber PDNS

Permasalahan yang ada pada pengelolaan PDNS yaitu *pertama*, belum adanya keseriusan pemerintah, khususnya Kemenkominfo RI dalam mempersiapkan pengamanan siber bagi PDNS. Ketidakseriusan itu ditunjukkan dengan belum ditindaklanjutinya permintaan Komisi I DPR RI agar ketika Kemenkominfo RI mulai menyiapkan PDNS, harus saat itu juga sistem pengamanannya sudah disiapkan. Keinginan untuk mengimplementasikan Satu Data Nasional belum diimbangi dengan pondasi infrastruktur pengamanan yang memadai. Belum adanya infrastruktur pengamanan siber bagi PDNS tersebut berimbas pada permasalahan *kedua*, yaitu ketidaksiapan SDM yang berkompeten dalam menghadapi serangan siber.

Namun demikian, kedua permasalahan inti tersebut sebetulnya juga perlu menjadi pengkajian internal bagi Komisi I DPR RI, mengingat penyediaan infrastruktur teknologi anti serangan siber pada PDNS dan penyiapan SDM yang profesional untuk mengoperasikan teknologi itu membutuhkan dukungan anggaran yang besar. Ketika mengingatkan Kemenkominfo RI dan BSSN tentang pentingnya infrastruktur teknologi anti serangan siber dan SDM profesional, Komisi I DPR RI mengakui bahwa anggaran yang betul-betul memadai untuk itu masih akan diperjuangkan. Dengan demikian, peristiwa ini seharusnya dapat mendorong Komisi I DPR RI untuk lebih gencar memperjuangkan anggaran bagi pengembangan teknologi dan penyiapan SDM, khususnya bagi BSSN.

Sebetulnya, ada satu hal lagi yang menjadi penyebab begitu mudahnya *hacker* menyerang PDNS, yaitu Kemenkominfo RI dan BSSN ternyata hanya mengandalkan *Windows Defender* yang merupakan produk "bawaan" dari Windows yang banyak dikeluhkan efektivitasnya dalam memproteksi data. Seharusnya, meskipun anggaran untuk pengadaan sistem teknologi pengamanan siber belum optimal, Kemenkominfo RI

dan BSSN menggunakan teknologi yang setidak-tidaknya lebih kuat atau lebih efektif daripada *Windows Defender*, misalnya *Linux*.

Direktur Jenderal Aplikasi Informatika Kemenkominfo RI Samuel Abrijani Pangerapan menyatakan ada data dari 210 instansi pemerintahan pusat ataupun daerah yang terdampak, contohnya adalah layanan keimigrasian di semua bandara internasional di Indonesia ("Keamanan Siber; Pemerintah Menolak Permintaan Peretas", 2024). Selain itu, layanan pembuatan paspor juga terganggu. Di Kantor Imigrasi Kelas I Khusus non-TPI Jakarta Barat, misalnya, pembuatan paspor yang semula hanya membutuhkan waktu 3-4 hari menjadi 7-8 hari ("Perlindungan Data Strategis Lemah", 2024). Namun, sejak 24 Juni 2024 pagi, sistem layanan publik milik Direktorat Jenderal Imigrasi mulai pulih, contohnya layanan *visa on arrival*.

Data milik Badan Intelijen Strategis (Bais) Tentara Nasional Indonesia (TNI) dan *Indonesia Automatic Fingerprint Identification System* (Inafis) Kepolisian Republik Indonesia (POLRI) juga termasuk di antara yang terdampak ("Keamanan Siber; Pemerintah Menolak Permintaan Peretas", 2024). Akun penyerang yang menamakan dirinya MoonzHaxor disebutkan telah mengunggah kiriman penjualan data Inafis POLRI seharga 1000 hingga 7000 dollar AS ("Serangan Siber; Sepekan Insiden PDN Belum Bisa Dipulihkan", 2024). Gangguan juga dialami Sistem Informasi Manajemen Sistem Penyediaan Air Minum (SIMSPAM) dan Sistem Informasi Infrastruktur Sanitasi Kementerian Pekerjaan Umum dan Perumahan Rakyat, serta Sistem Informasi Pengelolaan Keuangan Daerah Kementerian Dalam Negeri ("Keamanan Siber; Gangguan di Pusat Data Nasional Belum Dapat Diatasi", 2024).

Upaya yang Harus Dilakukan Pemerintah

Chairman Communication and Information System Security Research Center Pratama Persadha menilai bahwa proses desain PDNS dan PDN dilakukan secara tertutup oleh Kemenkominfo RI. BSSN juga tidak dilibatkan pada saat desain dilakukan. Pratama Persadha juga menyatakan bahwa pemerintah harus segera melakukan kajian serta audit dari desain PDN, baik dari sisi infrastruktur maupun dari sisi keamanannya ("Keamanan Siber; Pemerintah Menolak Permintaan Peretas", 2024). Kejadian ini akan lebih berbahaya jika peretas sampai dapat mengakses server di PDN dan membocorkan data ("Keamanan Siber; Gangguan di Pusat Data Nasional Belum Dapat Diatasi", 2024).

Di pihak parlemen, Ketua Komisi I DPR RI Meutya Hafid mengingatkan bahwa Kemenkominfo RI sebagai pengelola data wajib memastikan keamanan data yang dikelola sebagaimana amanat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Meutya Hafid juga menyayangkan bahwa pemerintah tidak kunjung membuat peraturan turunan dari UU PDP, terutama terkait pembentukan otoritas pengawas pengelola data pribadi ("Keamanan Siber; Pemerintah Menolak Permintaan Peretas", 2024).

Anggota Komisi I DPR RI Fraksi Partai Demokrasi Indonesia Perjuangan (PDIP) Tubagus Hasanuddin menyatakan bahwa insiden ini membuktikan bahwa kemampuan negara untuk memproteksi data strategis masih lemah. Ke depan, diharapkan pemerintah dapat menyiapkan infrastruktur pengamanan yang canggih dan segera melatih sumber daya manusia (SDM) di setiap lembaga negara agar memiliki kemampuan profesional

menangani security PDN. Tubagus Hasanuddin juga mengakui bahwa penyiapan hal-hal tersebut adalah tidak mudah karena keterbatasan keuangan negara ("Perlindungan Data Strategis Lemah", 2024).

Pengamat teknologi dan ahli forensik siber Ruby Alamsyah menyatakan bahwa pembangunan sistem PDNS belum dilengkapi dengan prosedur antisipasi terhadap gangguan atau serangan siber. Seharusnya, sistem PDNS ketika mulai dibangun harus segera diiringi dengan prosedur yang disebut *Business Continuity Plan* (BCP) atau *Disaster Recovery Plan* (DRP). PDNS belum memiliki sistem cadangan, padahal seharusnya sudah harus ada sokongan *Data Recovery Center* (DRC). Pemerintah seharusnya bisa memastikan back up sistem atau DRC aktif secara *real time*. Jadi, walaupun sistem utama mati, rusak, atau apa pun, baik karena fisik maupun karena *ransomware*, *back up system* dapat menyala kembali ("Keamanan Siber; Gangguan di Pusat Data Nasional Belum Dapat Diatasi", 2024). Mendesain jaringan dan kedisiplinan menjaga celah keamanan baru dengan melakukan *patch* teratur dan otomatis adalah hal-hal yang seharusnya dilakukan sebagaimana yang ditekankan oleh praktisi teknologi informasi Alfons Tanujaya ("Gangguan Pusat Data Nasional; Jika Terjadi Kebocoran Data, Pemerintah Harus Beri Tahu", 2024).

Selanjutnya, menurut pakar teknologi informasi dari Institut Teknologi Bandung (ITB) Basuki Suhardiman, seharusnya BSSN secepatnya melakukan kerja sama dengan negara lain yang sudah berpengalaman menghadapi serangan ransomware. Negara yang dapat diajak kerja sama misalnya Amerika Serikat (AS) yang sudah memiliki anti-enkripsi bagi serangan *ransomware* ("Audit Independen Proyek Pusat Data", 2024).

Namun demikian, masih ada faktor lain yang belum dibahas terkait lemahnya pengamanan PDNS terhadap serangan siber, yaitu faktor dasar hukum. Ternyata, dalam Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Perpres/39) belum ada muatan kewajiban yang tegas tentang keharusan mengembangkan teknologi pengamanan siber bagi PDNS. Hal-hal yang diatur antara lain hanya terkait definisi data dan penggunaannya.

Adapun dua hal yang menjadi permasalahan inti penyebab lemahnya keamanan SDI yaitu masalah infrastruktur teknologi pengamanan siber dan SDM profesional pendukungnya belum ada secara jelas. Satu-satunya pasal yang menyinggung masalah SDM hanyalah Pasal 29 ayat (2) Perpres Nomor 39 Tahun 2019 yang menyatakan bahwa rencana aksi Satu Data Indonesia dapat mencakup: "pengembangan sumber daya manusia yang kompeten", dan itu pun induk kalimatnya menggunakan kata "dapat", sehingga tidak mencerminkan kewajiban. Ketidaktegasan kewajiban menyediakan SDM profesional dalam mengamankan data itulah yang tampaknya menyebabkan Kemenkominfo RI dan BSSN merasa penyediaan SDM tersebut adalah sesuatu hal yang bukan merupakan prioritas utama dan dapat ditunda.

Penutup

Pada fungsi legislasi, Komisi I DPR RI perlu segera mengajukan RUU tentang Satu Data Indonesia. Hingga Juli 2024, Naskah Akademik dan draf

RUU tentang RUU tentang Satu Data Indonesia masih berada pada tahap uji konsep. Hal yang perlu diperhatikan adalah bahwa sebaiknya dalam RUU tidak hanya memuat aturan-aturan mengenai definisi dan pengelolaan data saja, tetapi juga harus memuat kewajiban bagi setiap lembaga negara untuk menyiapkan sistem pengamanan siber bagi PDNS dan menyediakan SDM yang profesional untuk menanganinya.

Pada fungsi pengawasan, Komisi I DPR RI perlu memantau perkembangan pembangunan sistem pengamanan siber bagi PDNS yang dilakukan oleh Kemenkominfo RI dan BSSN. Ketika kedua lembaga itu tidak menunjukkan keseriusan dalam hal itu, Komisi I DPR RI harus tegas memberikan peringatan keras, karena keamanan negara dipertaruhkan.

Referensi

Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu Data Indonesia (2019).

Fak/Wil/Nad. (2024, Juni 22). Perlindungan Data Strategis Lemah. *Kompas*, 3.

Dyt/Med/Cok. (2024, Juni 24). Keamanan Siber; Gangguan di Pusat Data Nasional Belum Dapat Diatasi. *Kompas*, 1 & 15.

Med/Ina/Nia/Bow/Dna/Edn. (2024, Juni 25). Keamanan Siber; Pemerintah Menolak Permintaan Peretas. *Kompas*, 1 & 15.

Zuhdi, Naufal. (2024, Juni 25). Audit Independen Proyek Pusat Data. *Media Indonesia*, 1.

Nia/Spw/Ndy/Nad. (2024, Juni 26). Gangguan Pusat Data Nasional; Jika Terjadi Kebocoran Data, Pemerintah Harus Beri Tahu. *Kompas*, 3.

Wil. (2024, Juni 27). Serangan Siber; Sepekan Insiden PDN Belum Bisa Dipulihkan. *Kompas*, 1 & 15.

Info Singkat

http://pusaka.dpr.go.id ISSN 2088-2351