ISU Sepekan

BIDANG HUKUM

Minggu ke-3 September 2021 (10 s.d. 16 September)

DUGAAN PERETASAN DATA 10 INSTANSI PEMERINTAH

Pusat Penelitian Badan Keahlian
Sekretariat Jenderal DPR RI

Sulasi Rongiyati, S.H., M.H.
Peneliti Ahli Madya/Hukum Perdata
sulasi.rongiyati@dpr.go.id

ISU ATAU PERMASALAHAN

Aksi peretasan jaringan internal diduga telah menyerang 10 (sepuluh) jaringan internal Kementerian/Lembaga, termasuk jaringan internal milik Badan Intelijen Negara (BIN). The Record, telah menginformasikan temuan peretasan berdasarkan temuan Insikt Group, divisi penelitian ancaman siber Recorded Future. Laporan Insikt menyebutkan pada April 2021 terdapat *malware* PlugX dari Mustang Panda di dalam Jaringan Pemerintah Indonesia. Mustang Panda merupakan kelompok peretas asal China yang dikenal dengan berbagai aksi spionase dengan target negara-negara di kawasan Asia Tenggara.

Peristiwa peretasan data 10 Kementerian/lembaga bukan yang pertama terjadi di Indonesia. Beberapa kasus kebocoran data pada jaringan internal Pemerintah sebelumnya pernah terjadi, antara lain peretasan terhadap: data sertifikat vaksinasi Presiden Joko Widodo; 1,3 juta identitas pengguna E-HAC Kementerian Kesehatan; identitas 279 pengguna BPJS; 91 juta data pengguna Toko Pedia oleh Shiny Hunter; dan 13 juta data pengguna Bukalapak oleh Ghosticplayers. Kasus tersebut relevan dengan data Badan Siber dan Sandi Negara (BSSN) yang menyebutkan selama Januari- Agustus 2021 ditemukan lebih dari 888,7 juta serangan siber yang sebagian besar berbentuk *malware*. Kebocoran data akibat *malware* paling banyak ditemukan di sektor Pemerintah (45,5 persen), disusul sektor keuangan (10,4 persen), telekomunikasi (10,4 persen), penegakan hukum (10,1 persen), transportasi (10,1 persen), dan BUMN 2,1 persen.

Maraknya serangan siber merupakan salah satu dampak dari tingginya tingkat pengguna internet. Data Hootsuite dalam ”Digital 2021” yang dikutip Kompas menyebutkan pada awal tahun 2021 pengguna internet Indonesia mencapai 102,6 juta jiwa atau menjangkau 73,7 persen penduduk. Jumlah ini melonjak jauh dari pengguna internet tahun 2002 yang baru mencapai 4,1 juta jiwa. Pemanfaatan teknologi informasi dan komunikasi digital yang tinggi berdampak pada risiko serangan siber dan keamanan data publik semakin rentan. Terlebih di era pandemi Covid-19, di mana sebagian besar aktivitas dilakukan melalui ruang siber. Demikian juga dengan adanya kebijakan Pemerintah Indonesia yang menerapkan sistem satu data, juga akan berpotensi meningkatkan risiko serangan siber.

Menyikapi dugaan peretasan jaringan internal Pemerintah oleh Mustang Panda, Pemerintah melalui BSSN perlu segera melakukan investigasi dugaan peretasan yang menyasar 10 Kementerian/Lembaga untuk mengungkap pelaku peretasan dan menjaga kepercayaan publik terhadap reputasi Pemerintah di ruang publik. Pemerintah juga perlu melakukan evaluasi dan pembenahan terhadap tata kelola keamanan siber Indonesia secara menyeluruh termasuk infrastruktur dan dibutuhkan peningkatan ketersediaan dan kemampuan sumber daya manusia (SDM).

Pakar Teknologi Informatika, Onno W Purbo mengungkapkan bahwa sistem keamanan jaringan internal Pemerintah Indonesia saat ini belum memadai. Salah satu sebabnya adalah keterbatasan SDM serta kualitas SDM yang belum dibekali dengan kemampuan untuk mengatasi serangan siber. Terlebih jika dikaitkan dengan keamanan siber membutuhkan audit keamanan informasi terhadap seluruh layanan publik.

Terkait tindak lanjut penanganan kasus peretasan jaringan internal Pemerintah, Kepolisian Republik Indonesia menyatakan telah berkoordinasi dengan Kemenkominfo untuk menindaklanjuti dugaan peretasan data tersebut. Namun, Kepolisian belum melakukan penyidikan karena masih berkoordinasi dengan pihak-pihak terkait lainnya, termasuk BSSN. Mengacu pada Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), penanganan insiden, termasuk peretasan, menjadi ranah kewenangan BSSN.
Secara umum, dasar hukum pengaturan keamanan siber di Indonesia adalah UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016 (UU ITE). UU ITE memberikan perlindungan hukum untuk konten sistem elektronik dan transaksi elektronik, tetapi tidak mencakup aspek penting keamanan siber, seperti infrastruktur informasi dan jaringan, serta SDM dengan keahlian di bidang keamanan siber. Sebagai peraturan pelaksana UU ITE diberlakukan PP PSTE yang mengatur penyelenggaraan keamanan siber pada sistem dan transaksi elektronik, namun hanya mencakup pengaturan kejahatan siber yang berhubungan dengan transaksi elektronik.

Peraturan pelaksana lainnya adalah Peraturan Kementerian Pertahanan Nomor 82 Tahun 2014 yang mengatur pedoman pertahanan siber. Peraturan itu merupakan satu-satunya peraturan yang menjabarkan definisi keamanan siber. Oleh karenanya pembentukan UU yang mengatur keamanan siber secara komprehensif menjadi sangat dibutuhkan. DPR RI Bersama Pemerintah telah mencantumkan RUU Pertahanan dan Keamanan Siber dalam Program Legislasi Nasional (Prolegnas) 2019-2024, namun sampai saat ini belum diprioritaskan untuk dibahas.

SUMBER

Kompas, 14 dan 15 September 2021; Media Indonesia, 14 September 2021; kominfo.go.id, 14 September 2021; lider.id, 13 September 2021; Kompas.com, 13 September 2021.