Isu Sepekan
Bidang Polhukam, Komisi I
Minggu ke-2 September
(8 s.d. 14 September 2022)
2022

Pusat Penelitian Badan Keahlian
Sekretariat Jenderal DPR RI

HACKER BJORKA DAN ANCAMAN KEMANAN SIBER

Aulia Fitri
Analis Legislatif Ahli Pertama
aulia.fitri@dpr.go.id

Isu dan Permasalahan

Kemunculan *hacker* Bjorka sejak bulan Agustus menambah daftar panjang serangan siber di Indonesia. Berawal dari kebocoran data 1,3 pengguna kartu SIM ponsel, Bjorka secara bertahap terus melakukan peretasan terhadap beberapa instansi pemerintahan dan tokoh-tokoh nasional. Perkembangan terbaru, Bjorka mengklaim telah berhasil meretas sejumlah dokumen kepresidenan sebanyak 679.180 data termasuk dokumen dari Badan Intelijen Negara (BIN). Sebelumnya, Bjorka meretas 105 juta data pemilih dari situs Komisi Pemilihan Umum (KPU) yang diperjualbelikan di situs *online*.

Dalam merespons kejadian ini, Kementerian Komunikasi dan Informatika menyatakan telah melakukan rapat koordinasi dengan berbagai pihak termasuk dengan Badan Siber dan Sandi Negara (BSSN). BSSN tengah melakukan penelusuran terhadap beberapa dugaan insiden peretasan data yang terjadi, serta melakukan validasi terhadap data-data yang dipublikasikan. Di lain pihak, BIN menyanggah adanya kebocoran data dan memastikan saat ini seluruh dokumen lembaganya dan Presiden masih terlindungi dengan baik.

Sejak awal tahun 2022 hingga saat ini terhitung sudah terjadi 10 kasus peretasan dan kebocoran data. Pada Januari 2022, grup *ransomware* Conti mencuri 228 GB data dari Bank Indonesia. Selain itu, terdapat kasus kebocoran data pasien di sejumlah rumah sakit di Indonesia yang dijual di forum *online* Raidforums. Kemudian pada Agustus 2022, 17 juta data pelanggan PLN bocor dan dijual di situs *breached.to* dan baru-baru ini 1,3 miliar data registrasi kartu SIM di Indonesia dijual di forum yang sama.

Beberapa kasus mengenai serangan siber yang terjadi menandakan ketergantungan negara terhadap teknologi informasi membawa tantangan dan ancaman tersendiri. Serangan siber didefinisikan sebagai serangan yang dilakukan baik oleh aktor negara maupun non negara menggunakan jaringan komputer, internet di ranah dunia maya dengan tujuan melakukan gangguan, pencurian data atau membuat kerusakan sistem komputer dan jaringan suatu negara, kelompok atau organisasi. Adapun bentuk serangan siber di antaranya: *hacking, cracking, ransomware* dan *cyber sabotage*. Bukan tidak mungkin, ancaman siber juga dapat terjadi terhadap pertahanan negara melalui *cyber terrorism* dan *cyber espionage*.

Indonesia memiliki pekerjaan rumah untuk mencegah berbagai kebocoran data dan peretasan, terutama di lembaga negara dan swasta yang memproses data pribadi masyarakat. Kejadian ini menunjukkan bahwa situs maupun akun medsos pemerintah sangat mudah untuk diretas. Sudah saatnya instansi pemerintahan diperkuat dengan panduan, sumber daya manusia, dan teknologi dengan kualitas yang mumpuni di bidang keamanan siber. Penting bagi pemerintah untuk melakukan investigasi menyeluruh atas peretasan beruntun yang terjadi belakangan ini. Sejauh ini, masih belum ada analisis dan tindakan yang bersifat komprehensif atas aksi serangan siber ini. Selain itu, dibutuhkan juga

mitigasi risiko yang menyeluruh oleh pemerintah dengan melibatkan para pemangku kepentingan di bidang keamanan siber seperti Kementerian Komunikasi Informatika, BSSN, BIN, Polri dalam ranah keamanan nasional serta TNI apabila ancaman siber telah tereskalasi menjadi ancaman pertahanan negara.

Semakin pesatnya perkembangan teknologi informasi berdampak pada risiko ancaman di ruang siber yang mendorong negara untuk menata kebijakan keamanan dalam merespons ancaman siber yang semakin nyata. Pencapaian kekuatan siber bergantung pada strategi dan kebijakan suatu negara dalam mengembangkan keamanan siber. Indonesia belum memiliki kebijakan khusus untuk mengelola dan menangani keamanan siber secara terintegrasi. Strategi keamanan siber yang kuat perlu diimbangi dengan dukungan hukum yang komprehensif dalam menghadapi ancaman keamanan siber. Penetapan regulasi yang tepat dan kerja sama semua pihak baik pemerintah, sektor swasta dan masyarakat sipil, dapat menjadi kunci dalam menghadapi tantangan dunia siber yang semakin kompleks.

Atensi DPR

Komisi I DPR melalui fungsi legislasi telah menunjukkan komitmennya dalam perlindungan data pribadi warga negara melalui Undang-Undang Perlindungan Data Pribadi yang akan segera disahkan. Selain itu, RUU tentang Keamanan dan Ketahanan Siber juga sudah masuk ke dalam Prolegnas 2020-2024 sebagai usul inisiatif DPR.

Komisi I melalui fungsi pengawasan dapat mendorong mitra kerja baik dalam upaya mitigasi maupun optimalisasi penanganan ancaman keamanan siber, termasuk bekerja sama dengan instansi terkait lainnya. Komisi I dapat mendorong Kementerian Komunikasi dan Informatika untuk bekerja sama dengan BSSN, BIN, Polri dalam ranah keamanan nasional serta TNI apabila ancaman siber telah tereskalasi menjadi ancaman pertahanan negara. Penguatan kerja sama dan koordinasi antarinstansi diperlukan untuk menangani keamanan siber secara terintegrasi.

Komisi I juga dapat menghimbau BIN untuk terus memantau dan memetakan potensi ancaman keamanan siber sebagai upaya mitigasi dan *early warning* terhadap pemerintah agar potensi ancaman siber dapat dicegah dan diatasi sebelum tereskalasi menjadi ancaman yang lebih serius.

Sumber

cnnindonesia.com, 12 September 2022;
detiknews.com, 12 September 2022;
kompas.com, 12 dan 13 September 2022;
republika.co.id, 13 September 2022;
tempo.co, 12 September 2022.

IsuSepekan

Koordinator Sali Susiana
Polhukam Puteri Hikmawati
Ekkuinbang Sony Hendra P.
Kesra Hartini Retnaningsih

https://puslit.dpr.go.id
@puslitbkd_official

EDITOR

Polhukam
Simela Victor M.
Prayudi
Novianto M. Hantoro

Ekkuinbang
Riyadi Santoso
Sri Nurhayati Q
Dian Cahyaningrum
Venti Eka Satya
Nidya Waras Sayekti

Kesra
Achmad Muchaddam F.
Yulia Indahri
Rahmi Yuningsih

LAYOUTER

Dewi Sendhikasari D.
Sita Hidriyah
Noverdi Puja S.
Anih S. Suryani
Teddy Prasetiawan
T. Ade Surya
Masyithah Aulia A.
Yosephus Mainake
Mohammad Teja
Nur Sholikah P.S.
Fieka Nurul A.