OPINI
Jika Anda ingin menyampaikan keluhan, kritik dan saran tentang pelayanan publik, silahkan mengirimkan melalui:
● Sekretaris Redaksi : (0711) 440088 ● Email : sriwijayapost@yahoo.com / redsripoku@gmail.com
Redaksi juga menerima artikel (opini) dan Mimbar Jumat maksimal 2 pages, diketik satu spasi, huruf Times New Roman (size: 12), dilengkapi foto diri (bukan pas foto)
Setiap artikel/tulisan/foto atau materi apapun yang telah dimuat di harian Sriwijaya Post dapat diumumkan/dialihwujudkan dalam format digital atau nondigital yang tetap merupakan bagian dari Harian Sriwijaya Post

Menjaga Kedaulatan Digital

OLEH:
Muhammad Syahri Ramadhan, S.H.,M.H
Ketua Pusat Kajian Hukum Sriwijaya (SLC) dan Dosen Fakultas Hukum Universitas Sriwijaya

KASUS peretasan Pusat Data Nasional (PDN) sungguh sangat membuat pilu semua pihak. Pemerintah yang dipercaya menjaga keamanan dan kenyamanan di dunia maya, tampak dibuat sibuk atas serangan virus ransomware saat ini. Berdasarkan data dari Kementerian Komunikasi dan Informatika (Kominfo), bahwa ada 282 data dari instansi pemerintah yang diserang oleh virus tersebut.

Meskipun, sudah ada beberapa situs yang sudah pulih kembali, tetapi masih ada sebagian data yang masih harus diperbaiki hingga saat ini.

Serangan masif terhadap situs pemerintah seyogianya jangan dipandang remeh. Fenomena ini justru dapat menjadi stigma di masyarakat dalam lingkup nasional bahkan internasional. Pemerintah mempunyai Pekerjaan Rumah (PR) besar dalam menjaga stabilitas digitalisasi di Indonesia.

Menjaga keamanan data nasional, tidak hanya berbicara tentang menjaga data pribadi setiap warga negara. Namun, hal ini juga berbicara menjaga jati diri bangsa dan merawat kedaulatan digital di bumi ibu pertiwi.

Memecah masalah kejahatan hacking yang terjadi saat ini, tidak semudah mengungkap kejahatan konvensional seperti pencurian, pembunuhan atau penganiayaan. Faktor eksistensi pelaku kejahatan yang keberadaannya tidak diketahui secara pasti, menjadi alasan betapa kompleksnya untuk menangkap pelaku tersebut.

Bahkan, banyak kasus kejahatan siber berupa hacking (peretasan), Penipuan Phsing, Cyber Stalking dan Cyber Bullying, dilakukan para oknum tersebut dengan menggunakan akun palsu. Belum lagi, permainan algoritma pemrograman para hacker untuk mengelabui lokasi keberadaan dari si pelaku tersebut. Hal itu membuat aparat penegak hukum harus ekstra kerja keras dalam mencari posisi pelaku.

Memperkuat Upaya Preventif

Kasus peretasan PDN sebenarnya bukanlah kasus kejahatan di dunia maya yang pertama kali terjadi. Pada tahun 2023, menurut kominfo terdapat 29 juta serangan siber yang diblokir di Indonesia. Beberapa kasus fenomenal terkait kejahatan siber pada tahun tersebut seperti dugaan bocornya data 34.900.867 paspor Warga Negara Indonesia (WNI), kasus peretasan perbankan yaitu bocornya data dari Bank Syariah Indonesia (BSI), 16,5 juta data Pengguna BPJS Ketenagakerjaan yang diretas lalu dijual di forum gelap seharga 153 juta rupiah dan kasus peretasan terkait 337 juta data di Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) Kemendagri (Jay Sadikin Abdul Azis Mandala Putra, 2024: 26).

Dalam lingkup global, kasus peretasan juga acapkali terjadi di hampir setiap tahun nya. Adapun berbagai contoh kasus seperti Sony Pictures sebagai salah satu perusahaan film terkemuka di dunia, diretas data nya oleh hacker yang diduga dari Korea Utara. Lalu, peretasan terhadap situs Pentagon (Kementerian Pertahanan Amerika Serikat, Kasus Wikileaks (Edward Snowden), lalu kasus penyadapan yang dialami oleh Presiden Ke-6 Indonesia Susilo Bambang Yudhoyono (SBY) oleh Australia dan Selandia Baru (Agus Subagyo, 2015: 97).

Polemik terhadap kejahatan dunia maya yang terjadi dalam lingkup nasional maupun internasional sudah seharusnya menjadi bahan refleksi bagi setiap negara, tak terkecuali Indonesia. Diperlukan evaluasi secara menyeluruh terhadap perangkat teknologi mulai dari perangkat software (perangkat lunak) maupun hardware (perangkat fisik).

Perhatian pemerintah terhadap dunia siber seyogianya sangat intens. Hal ini dibuktikan besarnya anggaran yang digelontorkan untuk membuat berbagai aplikasi. Sebagaimana diketahui, untuk tahun ini saja pemerintah mengeluarkan anggaran di kisaran 6,2 triliun terkait pembuatan platform dan aplikasi baru. Lalu, terdapat 27 ribu aplikasi yang dibuat baik dari instansi pemerintah pusat maupun daerah.

Meskipun di sisi lain, membludaknya aplikasi tersebut justru berefek kepada saling tumpang tindih dalam pelayanan birokrasi. Mengingatnya besarnya biaya yang dikeluarkan oleh pemerintah, sudah sepatutnya pengelolaan situs pemerintah harus dioptimalkan sebaik mungkin baik dari aspek upaya preventif maupun represifnya.

Kebijakan dalam pembuatan aplikasi atau situs instansi, jangan hanya dilihat dari aspek kuantitas yaitu seberapa banyak jumlah platform yang sudah dibuat. Faktor kualitas juga harus diperhatikan, terutama dari segi keamanan data pribadi maupun kenyamanan penggunanya yang pada umumnya masyarakat itu sendiri.

Ribuan situs yang dimiliki negara saat ini, justru dikhawatirkan menjadi buah simalakama. Dengan maksud memberantas pungli, menciptakan pelayanan birokrasi yang simpel dan tidak berbelit – berbelit. Namun, pada saat berbagai situs dibuat, justru masalah baru lagi yang ditimbulkan yaitu terjadinya serangan siber dari para hacker.

Dari sisi regulasi, Indonesia sudah meresponnya dengan menerbitkan beberapa peraturan perundang – undangan yang berkaitan dengan aktivitas di dunia maya seperti UU No. 8 tahun 2011 tentang Informasi dan Transaksi Elektronik dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Namun, mengatasi problematika dunia virtual tidak cukup berpedoman kepada aspek substansi (peraturan) hukum saja. Aspek aparat penegak hukum (struktur hukum) dan budaya hukum harus juga diperhatikan secara komprehensif.

Pola penegakan hukum terkait kejahatan siber masih didominasi kepada orientasi upaya represif dibandingkan preventif. Padahal, upaya represif tidak sekedar menangkap pelaku kejahatan saja. Tindakan manipulatif dari para hacker ini memberikan kerugian yang sangat besar, seyogianya harus diantisipasi sebelum terjadinya serangan.

Salah satu contoh ialah peretasan yang dialami situs di bawah naungan Kementerian Pendidikan dan Kebudayaan (Kemdikbud), bahwa terdapat 800 ribu data calon mahasiswa pendaftar Kartu Indonesia Pintar Kuliah (KIP-Kuliah) ikut hilang sebagai akibat dari gangguan Pusat Data Nasional (emedia.dpr.go.id).

Hilangnya data calon mahasiswa tersebut tentunya akan memberikan efek domino terhadap kelangsungan kegiatan perkuliahan mengingat aspek finansial (ekonomis) merupakan salah satu faktor pendukung sarana dan prasarana demi menjaga kelancaran kegiatan perkuliahan di instansi perguruan tinggi. Tidak hanya mahasiswa, pihak kemdikbud pun harus kerepotan untuk mencari dan merekapitulasi data calon mahasiswa tersebut.

Maka dari itu, upaya preventif harus dikedepankan dalam menangani permasalahan di Bidang Teknologi Informasi dan Komunikasi. Semua pihak mulai dari Kepolisian, Kominfo, Badan Siber dan Sandi Negara, dan berbagai institusi terkait (stakeholder), harus berkoordinasi dan berkolaborasi dalam mencegah serangan siber untuk periode selanjutnya.

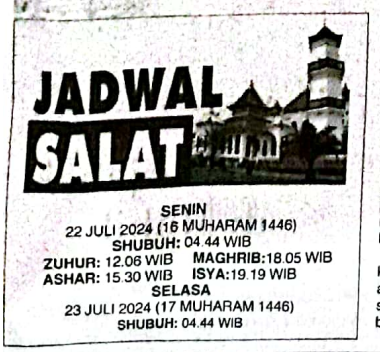
Salah satu upaya preventif tersebut seperti pemanfaatan backup data nasional. Sebagaimana disampaikan oleh Kominfo, hanya 2 persen data backup di Pusat Data Nasional. Hal ini harus menjadi cambuk bagi institusi untuk lebih mengoptimalkan setiap perangkat software yang sudah disediakan pemerintah.

Upaya lainnya ialah setiap instansi terkait harus selalu melakukan upgrade dalam kemampuan bidang teknologi informasi dan komunikasi. Para hacker yang melakukan kejahatan siber, merupakan oknum yang selalu meningkatkan kemampuan dalam melakukan pemrograman. Maka dari itu, upaya deteksi dini terhadap kemungkinan serangan siber yang tidak mengenal waktu, dapat dilakukan jika kemampuan aparatur di setiap institusi juga berada dalam level kelas wahid.

Seperti adagium yang terkenal dalam dunia kesehatan, bahwa mencegah lebih baik daripada mengobati. Alangkah baiknya potensi bahaya hacking dapat ditanggulangi sebelum adanya serangan ransomware yang merugikan keamanan ratusan situs pemerintah saat ini. Tertaksananya upaya preventif dan represif secara proposional, merupakan suatu kunci dalam menjaga kedaulatan digital di Indonesia. (*)

Menjaga keamanan data nasional, tidak hanya berbicara tentang menjaga data pribadi setiap warga negara. Namun, hal ini juga berbicara menjaga jati diri bangsa dan merawat kedaulatan digital di bumi ibu pertiwi. Memecah masalah kejahatan hacking yang terjadi saat ini, tidak semudah mengungkap kejahatan konvensional seperti pencurian, pembunuhan atau penganiayaan. Faktor eksistensi pelaku kejahatan yang keberadaannya tidak diketahui secara pasti, menjadi alasan betapa kompleksnya untuk menangkap pelaku tersebut. Bahkan, banyak kasus kejahatan siber berupa hacking (peretasan), Penipuan Phsing, Cyber Stalking dan Cyber Bullying, dilakukan para oknum tersebut dengan menggunakan akun palsu. Belum lagi, permainan algoritma pemrograman para hacker untuk mengelabui lokasi keberadaan dari si pelaku tersebut. Hal itu membuat aparat penegak hukum harus ekstra kerja keras dalam mencari posisi pelaku.

Pola penegakan hukum terkait kejahatan siber masih didominasi kepada orientasi upaya represif dibandingkan preventif. Padahal, upaya represif tidak sekedar menangkap pelaku kejahatan saja. Tindakan manipulatif dari para hacker ini memberikan kerugian yang sangat besar, seyogianya harus diantisipasi sebelum terjadinya serangan. Salah satu contoh ialah peretasan yang dialami situs di bawah naungan Kementerian Pendidikan dan Kebudayaan (Kemdikbud), bahwa terdapat 800 ribu data calon mahasiswa pendaftar Kartu Indonesia Pintar Kuliah (KIP-Kuliah) ikut hilang sebagai akibat dari gangguan Pusat Data Nasional (emedia.dpr.go.id). Hilangnya data calon mahasiswa tersebut tentunya akan memberikan efek domino terhadap kelangsungan kegiatan perkuliahan mengingat aspek finansial (ekonomis) merupakan salah satu faktor pendukung sarana dan prasarana demi menjaga kelancaran kegiatan perkuliahan di instansi perguruan tinggi. Tidak hanya mahasiswa, pihak kemdikbud pun harus kerepotan untuk mencari dan merekapitulasi data calon mahasiswa tersebut.



HARIAN UMUM
SRIWIJAYA POST
Penerbit: PT Sriwijaya Pordana SIUPP No 213/SK/Menpen/SIUPPA 2/1987 tanggal 22 Juni 1987 Jo. 186/Ditjen
DIREKTUR UTAMA: Dahlan Dahi, PEMIMPIN UMUM: Dahlan Dahi, KEPALA NEWS ROOM SRIWIJAYA POST-TRIBUN SUMSEL/ PEMIMPIN REDAKSI: Yudie Thirzano, WAKIL PEMIMPIN REDAKSI: Prawira Maulana, MANAJER PRODUKSI: Sugeng Haryadi, MANAJER ONLINE: Sudarwan, STAF REDAKSI: Wiedarto, Leni Juita, H Muhammad Husin, Abdul Hafiz, Tarso, Ardani Zuri, Hendra