

Waspada! Isu Hacker China Berpotensi Memecah Belah Bangsa

written by Muallifah



Harakatuna.com - Problem atas konsekuensi yang ditimbulkan dari kecanggihan teknologi, semakin hari kian marak. Baru-baru ini, masalah kebocoran data menjadi masalah yang marak dibicarakan. Jika mengingat masalah semacam ini, persoalan kebocoran data mulai menjadi pembicaraan serius ketika data kelolaan Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan diduga terbobol hacker China. Bulan Agustus lalu, sekitar 1,3 juta data pengguna aplikasi Health Alert Card (eHAC) buatan Kementerian Kesehatan Indonesia yang memuat data COVID-19 dibobol.

Terbaru, ada dugaan pembobolan data terhadap 10 kementerian dan lembaga oleh hacker China. Masalah ini kemudian memunculkan reaksi ketidasisigapan pemerintah dalam melindungi data pribadi rakyatnya.

Badan Intelijen Negara menanggapi secara tegas masalah ini dengan respon

bahwa sejauh ini servernya masih aman terkendali. Hal ini diungkapkan oleh Deputy VII BIN Wawan Hari Purwanto,

“Hingga saat ini server BIN masih dalam kondisi aman terkendali dan tidak terjadi hack sebagaimana isu yang beredar bahwa server BIN diretas hacker asal China,” ujar Wawan, dalam keterangan tertulis, Selasa (14/9/2021).

Masalah ini sebenarnya adalah akibat yang ditimbulkan dari semakin mudahnya akses pengetahuan, ruang bebas yang diciptakan oleh teknologi serta akibat canggihnya teknologi yang membuat orang lain dengan pengetahuannya bisa mengakses berbagai hal, termasuk mencuri secara digital, dan menjadi hantu digital dengan menimbulkan kecemasan-kecemasan dalam kelompok masyarakat, khususnya negara. Bagaimana masalah ini bisa terjadi? Bagaimana posisi kedaulatan siber di [Indonesia](#)? Bagaimana upaya pemerintah?

Berpotensi Memecah Bangsa

Dugaan kebocoran ini tidak hanya memicu keresahan masyarakat tentang data pribadi yang diakses oleh orang tidak dikenal dan dimanfaatkan secara sembarangan. Lebih jauh, masalah ini memicu pecah belah bangsa. Ketidakpercayaan keamanan data terhadap pemerintah, perlindungan akun dari masyarakat kepada pemerintah semakin tinggi ketika para buzzer, kelompok yang tidak pro terhadap pemerintah mulai menggencarkan aksinya untuk menebarkan informasi yang tidak benar kepada khalayak.

Akhirnya, dengan literasi digital, literasi baca yang cukup rendah, informasi-informasi tidak benar dengan tujuan provokator dikhawatirkan membuat masyarakat tergiring untuk bersikap reaktif dengan ketidaksiapan pemerintah dalam melindungi data dan merugikan negara Indonesia ketika diakses oleh orang lain, khususnya oleh hacker.

Tabayyun dalam Menerima Informasi

Menyikapi informasi ini, kita tidak perlu langsung merespons dengan reaktif dengan berbagai alasan yang menjadi pembenaran. Informasi kebocoran data ini seharusnya perlu ditelaah lebih jauh untuk oleh kita untuk melihat kebenaran fakta yang sebenarnya agak tidak mudah ikut arus komentar dan sikap reaktif yang ditunjukkan oleh beberapa kelompok.

Dalam menyikapi masalah ini, setidaknya beberapa fakta yang harus diketahui oleh kita diantaranya: masalah ini adalah hal yang wajar terjadi pada lembaga, Badan Intelijen Negara terus mendalami masalah ini, pengecekan berkala dengan data yang sudah ada, masyarakat tidak mudah percaya serta hacker yang berusaha mengutak-atik data pada 10 lembaga yang diduga kebocoran data tersebut bernama "Mustang Panda", peretas atau hacker asal China menggunakan *private* ransomware bernama Thanos.

Dengan mengetahui fakta-fakta di atas, setidaknya sikap tabayun terus diupayakan pada diri kita dalam menerima informasi, khususnya informasi yang erat kaitannya dengan potensi masalah kerusakan, perpecahan antar kelompok, menimbulkan ketidakpercayaan terhadap pemerintah, serta informasi apa pun yang berpotensi merusak keutuhan NKRI. Sikap tidak tergesa-gesa dalam menerima informasi semacam ini diiringi oleh kecerdasan digital, menelaah informasi dari berbagai sumber ditambah upaya-upaya lainnya.

Tidak berhenti pada sikap tabayun, pihak pemerintah juga harus memastikan bahwa tidak akan terjadi kebocoran data dengan melakukan berbagai upaya untuk kedaulatan siber Indonesia. Masalah ini menjadi masalah serius karena akan merugikan Indonesia.

Dengan demikian, upaya preventif yang seharusnya dilakukan oleh pihak pemerintah dengan dugaan hacker yang terus mengintai, harus dibekali dengan talenta terbaik untuk melindungi data yang ada agar tidak bisa diakses secara sembarangan. Pemerintah harus sigap dan lebih berhati-hati akan potensi masalah yang cukup serius ini. Sistem keamanan siber harus diciptakan sangat seideal mungkin agar tidak mudah diakses oleh hacker. Masalah kebocoran data yang terjadi sebelumnya, jangan sampai terjadi lagi, untuk alasan apa pun.
Wallahu a'lam