



Judul : Ketahanan siber dipertanyakan
Tanggal : Jumat, 28 Mei 2021
Surat Kabar : Republika
Halaman : 1 dan 9

Ketahanan Siber Dipertanyakan

■ NAWIR ARSYAD AKBAR, MIMI KARTIKA

JAKARTA — Belum usai kasus kebocoran data peserta BPJS Kesehatan, kini giliran sistem peringatan dini Badan Meteorologi Klimatologi dan Geofisika (BMKG) yang bermasalah. Kejadian itu pun menimbulkan pertanyaan dari berbagai kalangan mengenai ketahanan siber nasional.

Pada Kamis (27/5), beredar informasi melalui SMS *blast* BMKG-Kemenkominfo yang berisi perkiraan gempa bumi berkekuatan magnitudo 8,5 di sejumlah daerah dan berpotensi tsunami. BMKG telah menyatakan informasi tersebut tidak benar karena terjadi kesalahan sistem.

Anggota Komisi I DPR dari Fraksi Partai Keadilan Sejahtera (PKS), Sukamta, menyayangkan terjadinya kebocoran data BPJS dan kesalahan informasi dalam sistem BMKG. Menurut dia, permasalahan itu mengindikasikan lemahnya ketahanan siber di Indonesia. Ia meminta pemerintah segera melakukan mitigasi terhadap hal-hal yang berpotensi bermasalah di sektor teknologi informasi dan komunikasi. Palsunya, bocornya data hingga kesalahan informasi BMKG membuat masyarakat khawatir.

"Harus ada langkah-langkah ke depannya agar hal seperti ini tidak terjadi lagi. Ini penting untuk digarisbawahi karena sepertinya akan ada lagi kasus-kasus kebocoran data yang lebih parah," kata Sukamta, Kamis (27/5).

Menurut Sukamta, masalah-masalah tersebut menjadi tanda pentingnya rancangan undang-undang perlindungan data pribadi (RUU PDP). Salah satu pembahasannya mengenai lembaga yang mengurus data pribadi, apakah oleh Kementerian Komunikasi dan Informatika (Kemenkominfo) atau membentuk lembaga independen baru. "Ini harus segera *ketemu* kesepakatannya agar upaya perlindungan data pribadi bisa segera memiliki payung hukum yang kuat terhadap masyarakat, termasuk juga badan publik," ujar Sukamta.

Hal senada diungkapkan anggota Komisi I DPR Fraksi Partai Golkar, Dave Laksono. Ia



Ketahanan Siber Dipertanyakan dari hlm 1

menilai, kebocoran data menjadi tanda bahwa sistem pengamanan di Indonesia masih sangat rentan diretas. Hal tersebut tentu akan sangat berbahaya karena data-data tersebut dapat disalahgunakan oleh oknum-oknum tak bertanggung jawab.

"Kami di Komisi I ingin segera selesai karena masih banyak juga undang-undang lain yang perlu segera dirampungkan," ujar Dave.

Peneliti keamanan siber dari Communication Information System Security Research Center (CISSReC), Pratama Persadha, menilai dampak dari kesalahan SMS *blast* BMKG tak hanya menimbulkan kepanikan di masyarakat, tapi juga berpotensi menyebabkan kebocoran data. Risiko kebocoran data, kata dia, bergantung pada server yang diretas apakah menyimpan data-data pribadi penduduk atau tidak.

"Kalau ada, ya berpotensi sekali. Namun, menurut saya, dengan adanya daftar nomor ponsel yang dikirim melalui SMS, itu sudah merupakan data-data pribadi," kata Pratama kepada *Republika*, kemarin.

Untuk mencegah kesalahan terulang, Pratama menyarankan BMKG melakukan audit secara menyeluruh dan forensik digital mengenai keamanan informasi atas kesalahan SMS *blast* terkait perkiraan gempa bumi. Ketika ditanya mengenai penyebab kesalahan SMS *blast*, Pratama menyebutkan ada dua kemungkinan.

"Agak susah juga menebak, ini yang diretas dari sistemnya BMKG

atau sistemnya pemilik layanan SMS *blast* yang disewa BMKG," ujar Pratama.

Menurut dia, kemungkinan peretasan bisa terjadi pada sistem pengiriman SMS. Namun, kata Pratama, kesalahan atau sumber kerentanan mungkin bukan berasal dari BMKG, melainkan pemilik layanan SMS *blast*.

Karena itu, kata dia, sangat penting bagi BMKG melakukan audit untuk mencari penyebab terjadinya SMS *blast* yang memberikan informasi *hoaks* atas perkiraan gempa bumi dan potensi tsunami. BMKG harus meningkatkan keamanan sistem informasi, baik dari sisi teknologi komputasi, sumber daya manusia, maupun kebijakannya.

Menurut dia, perlu dicek juga perusahaan pengiriman SMS *blast* yang digunakan dalam pengiriman informasi BMKG. "Jangan-jangan malah mereka yang kecolongan," kata dia.

Selain itu, proses perbaikan sistem sebaiknya dilakukan di server uji coba dahulu, sebelum ke *live server*. Dengan demikian, apabila terjadi masalah dalam perbaikan tersebut tidak berefek ke *live system*.

Setelah meyakini perbaikan telah berhasil di server uji coba, barulah diimplementasikan ke *live server*. Selain jaringan BMKG sendiri, kata dia, perlu dicek juga jaringan kerja samanya, seperti jaringan Kementerian Komunikasi dan Informatika atau pemilik layanan SMS *blast*.

"Perlu dicek *log admin* pengguna SMS *blast*, supaya bisa diketahui lewat

celah mana sistem ini dimanfaatkan *hacker*," ujar Pratama.

Juru Bicara Kementerian Komunikasi dan Informatika Dedy Permadi mengklaim tidak ada peretasan di saluran komunikasi kerja sama Kementerian Kominfo-BMKG. Hal tersebut, Dedy menegaskan, untuk merespons dugaan adanya peretasan yang menjadi penyebab kesalahan sistem pengirim informasi SMS *blast* BMKG. "Tidak ada peretasan di sistem Kemenkominfo," kata Dedy saat dikonfirmasi, Kamis (27/5).

Namun, Dedy tidak menjelaskan lebih lanjut mengenai penyebab pasti dari kesalahan sistem SMS *blast* BMKG. Menurut dia, persoalan teknis merupakan kewenangan BMKG. "Terkait teknis masalahnya bisa ditanyakan ke BMKG karena konten langsung dikoordinasikan BMKG kepada operator seluler," kata Dedy.

BMKG melalui siaran pers menyatakan, SMS berisi perkiraan gempa bumi berkekuatan M 8,5 dan berpotensi tsunami tidak benar. "Informasi tersebut tidak benar karena telah terjadi kesalahan pada sistem pengiriman informasi gempa bumi dan peringatan dini tsunami melalui kanal SMS," ujar Kepala Pusat Gempa Bumi dan Tsunami BMKG Bambang Setiyo Prayitno dalam keterangannya di Jakarta, Kamis.

"Saat ini BMKG bersama Kemenkominfo sedang melakukan penelusuran dan investigasi lebih mendalam terhadap penyebab kesalahan sistem SMS hingga tersebar informasi gempa berpotensi tsunami," kata dia.

■ rr laeny sulistyawati/fauziah mursid
ed: satria kartika yudha