Geger Pemerintah Pasrah sama Hacker? Menguak Dampak dan Implikasi Serangan Siber di PDN

Sopiyan Hadi - TANGERANG.AWDI.OR.ID

Jun 27, 2024 - 20:59

OPINI - Dalam beberapa hari terakhir, serangan siber telah menjadi bukti

ancaman nyata bagi banyak negara di dunia, termasuk Indonesia. yang mengalami serangan ransomware Brain Cipher.

Pemerintah, sebagai pengelola utama data nasional (PDN) 2 di Surabaya, menjadi salah satu target utama serangan ransomware Brain Cipher ini. Meski demikian, Pemerintah memastikan bahwa PDN yang sedang dibangun di Cikarang, Jawa Barat, tidak terpengaruh oleh serangan ini.

Wakil Menteri Komunikasi dan Informatika (Wamenkominfo) Nezar Patria mengatakan bahwa PDN terus berjalan pembangunannya dan tidak ada dampak dari serangan siber. Hal ini diperkuat oleh Kepala Badan Siber dan Sandi Negara (BSSN) Hinsa Siburian yang memastikan bahwa PDN di Cikarang tidak memiliki hubungan dengan gangguan PDNS 2.

Meski demikian, kasus serangan siber ini dijadikan sebagai pelajaran untuk pengelolaan pusat data dan para pemilik data di Indonesia. Serangan ini merupakan varian terbaru dari Lockbit 3.0 yang baru muncul baru-baru ini. Hinsa menekankan bahwa ini perlu diketahui sebagai cara untuk mengantisipasi hal serupa di tempat-tempat lain.

Pemerintah juga fokus pada tanggapan dampak serangan siber terhadap layanan publik. Mereka akan evaluasi sistem keamanan dan segala macamnya untuk memitigasi kemungkinan serangan siber di masa depan. Dengan demikian, Pemerintah berusaha untuk memantapkan sistem keamanan dan mengantisipasi serangan siber yang lebih lanjut.

Dalam hal ini, Pemerintah Indonesia harus lebih peduli dengan isu keamanan siber. Serangan siber yang beruntun dan bertubi-tubi menunjukkan kurang pedulinya pemerintah terkait isu keamanan siber. Reputasi serta nama baik negara Indonesia akan tercoreng di mata dunia jika tak mampu mengantisipasi serangan yang terjadi.

Pemerintah harus lebih proaktif dalam mengantisipasi dan menghadapi serangan siber. Mereka harus meningkatkan sistem keamanan dan mengembangkan strategi yang lebih efektif untuk menghadapi serangan siber.

Dengan demikian, Pemerintah dapat memantapkan sistem keamanan dan mengantisipasi serangan siber yang lebih lanjut. Banyak yang bertanya-tanya, apakah pemerintah sudah pasrah menghadapi situasi ini? Atau apakah ada langkah konkret yang sedang diambil untuk mengatasi dan mencegah serangan siber di masa depan?

Serangan Siber: Ancaman Nyata bagi Keamanan Data Nasional

Serangan siber bukanlah hal baru, namun intensitas dan kompleksitas serangan terus meningkat.

Dalam beberapa kasus, serangan siber berhasil menembus pertahanan sistem informasi pemerintah, mengakses data sensitif, dan mengganggu layanan publik. Dampak dari serangan ini bisa sangat merusak, mulai dari kebocoran data pribadi hingga potensi ancaman terhadap keamanan nasional.

Salah satu serangan yang paling mencolok adalah ransomware, di mana

penyerang mengenkripsi data korban dan menuntut tebusan untuk memulihkan akses. Serangan seperti ini tidak hanya menyebabkan kerugian finansial tetapi juga mengancam kepercayaan publik terhadap kemampuan pemerintah dalam melindungi data mereka.

Mengapa Pemerintah Terlihat Pasrah?

Ada beberapa alasan mengapa masyarakat mungkin merasa bahwa pemerintah pasrah menghadapi ancaman ini. Pertama, kurangnya transparansi dalam menangani insiden keamanan siber seringkali membuat publik merasa pemerintah tidak cukup serius dalam menanggapi ancaman ini.

Informasi tentang serangan siber seringkali baru diketahui publik setelah dampaknya dirasakan luas, tanpa adanya pemberitahuan atau tindakan preventif sebelumnya.

Kedua, keterbatasan sumber daya manusia dan teknologi juga menjadi faktor penghambat. Banyak instansi pemerintah masih menggunakan sistem teknologi yang usang dan kurang dilengkapi dengan protokol keamanan yang memadai. Hal ini membuat mereka menjadi target empuk bagi penyerang yang terus mengembangkan metode serangan mereka.

Langkah-Langkah yang Diperlukan untuk Meningkatkan Keamanan Siber:

Meski terlihat pasrah, pemerintah sebenarnya telah melakukan beberapa langkah untuk memperkuat keamanan siber. Namun, ada beberapa langkah tambahan yang perlu dipertimbangkan untuk meningkatkan efektivitas upaya ini:

- Meningkatkan Infrastruktur Keamanan: Pemerintah perlu mengalokasikan anggaran yang memadai untuk memperbarui infrastruktur teknologi dan meningkatkan protokol keamanan. Investasi dalam teknologi keamanan terbaru dan infrastruktur yang lebih tahan terhadap serangan siber adalah langkah penting.

- Pelatihan dan Pengembangan SDM: Sumber daya manusia yang kompeten dalam bidang keamanan siber sangat diperlukan. Pemerintah harus mengadakan pelatihan reguler untuk pegawai dan bekerja sama dengan institusi pendidikan untuk mengembangkan kurikulum yang fokus pada keamanan siber.

- Kolaborasi dengan Sektor Swasta: Kerja sama dengan sektor swasta, termasuk perusahaan teknologi dan lembaga riset, dapat membantu pemerintah mengakses teknologi dan pengetahuan terbaru dalam menghadapi ancaman siber. Kolaborasi ini juga dapat membuka jalan untuk berbagi informasi tentang ancaman dan tren terbaru dalam keamanan siber.

- Meningkatkan Kesadaran Publik: Kampanye kesadaran tentang keamanan siber harus digalakkan untuk mengedukasi masyarakat tentang pentingnya perlindungan data pribadi dan cara-cara sederhana untuk melindungi diri dari ancaman siber.

- Regulasi dan Kebijakan yang Ketat: Pemerintah perlu memperkuat regulasi terkait keamanan siber, termasuk mengatur standar keamanan untuk instansi pemerintah dan sektor swasta. Penegakan hukum yang tegas terhadap pelaku

serangan siber juga sangat penting untuk menciptakan efek jera.

Peran Masyarakat dalam Meningkatkan Keamanan Siber:

Selain pemerintah, masyarakat juga memiliki peran penting dalam menjaga keamanan siber. Kesadaran akan pentingnya keamanan digital dan penerapan langkah-langkah sederhana seperti menggunakan kata sandi yang kuat, mengupdate perangkat lunak secara berkala, dan berhati-hati terhadap email phishing, dapat membantu mengurangi risiko serangan siber.

Serangan siber adalah ancaman serius yang memerlukan respon cepat dan tepat dari pemerintah.

Meski terlihat pasrah, upaya untuk meningkatkan keamanan siber terus dilakukan, meskipun masih banyak tantangan yang harus dihadapi.

Kerja sama antara pemerintah, sektor swasta, dan masyarakat adalah kunci untuk menghadapi ancaman ini secara efektif.

Dengan langkah-langkah yang tepat, diharapkan keamanan data nasional dapat terjaga dan kepercayaan publik terhadap kemampuan pemerintah dalam melindungi data mereka dapat kembali pulih.

Penulis: Muhammad Iqbal Saputra (Mahasiswa UIN Raden Mas Said Surakarta)