Dr. Pratama Persadha: UU PDP Belum Efektif, Ini Potensi Ancaman Siber 2023

Updates. - AC.WEB.ID

Dec 28, 2022 - 09:41

Dr. Pratama Persadha, Chairman CISSReC

JAKARTA - Tahun 2022 terbukti menjadi tahun penuh disrupsi di seluruh dunia di berbagai lini. Akibatnya, banyak negara terpaksa dengan cepat memprioritaskan kembali terhadap keamanan siber dan data. Dengan semakin dekatnya tahun 2023, pemerintah serta semua elemen masyarakat tanah air harus terus beradaptasi dengan perubahan kondisi kesehatan, politik, dan teknologi maupun tren kebocoran data yang mempengaruhi keamanan tiap individu.

Dalam keterangannya Rabu (28/12), pakar keamanan siber Pratama Persadha menjelaskan secara umum serangan siber di 2023 akan berkisar pada 3 hal, yaitu APT (Advanced Persisten Threat), ransomware dan supply chain attack. Serangan APT seringkali adalah bentuk serangan state actor seperti serangan APT-29 dari Rusia seperti dituduhkan AS dan sekutunya.

“Perang siber masih berlangsung dan mungkin semakin besar dengan kesepakatan bantuan serta pembelian senjata antara Ukraina dan Amerika Serikat. Tentu perang konvensional saat ini selalu disertai dengan perang siber yang sebenarnya juga sudah dan sednag berlangsung saat ini,” jelas chairman Lembaga Riset Keamanan Siber CISSReC (Communication and Information System Security Research Center) ini.

Ditambahkan Pratama, ransomware dan malware juga masih menjadi momok masyarakat global, lebih dari 30?ntuk serangan siber adalah dengan malware dan ransomware. Indonesia bahkan sudah pernah menjadi korban dengan motif politik dalam kasus email diplomat Kemlu ke pejabat Australia. Dimana ternyata email diplomat Kemlu telah diretas hacker asal Tingkok lalu, file email yang dikirim ke pajabat Australia mengandung malware Bodi Arya.

“Peristiwa tersebut menjadi bukti bagaimana kita masih jauh dari ideal soal pengamanan siber. Sistem cegah dini harus terus ditingkatkan sehingga kemampuan mendeteksi dan mitigasi serangan bisa lebih baik lagi. Bahkan kita tahu ada serangan setelah Australia mendeteksi adanya email yang mengandung malware, artinya pengamanan Australia bisa dibilang lebih baik dari Indonesia,” tegas Pratama.

Ancaman lain di 2023 yang meningkat adalah supply chain attack. Ini telah menjadi tren global ditengah arus globalisasi dan digitalisasi yang terus membesar. Artinya, pengawasan terhadap keamanan para vendor ini harus menjadi perhatian serius dari pemerintah, jangan sampai vendor membawa malware atau membuka celah keamanan baru tanpa mereka sadari.

“Supply chain attack di negara maju sudah menjadi perhatian serius, bahkan di AS Pentagon membuat aturan ketat soal keamanan siber setiap vendor yang bekerja bersama lembaga pertahanan dan keamanan di AS. Di Indonesia ini belum menjadi perhatian serius, padahal tidak sedikit vendor yang menggunakan produk dan teknologi asing. Ini jelas terbuka adanya kerangan siber dengan modus supply chain attack,” jelas pria yang juga Dosen S3 PTIK ini.

Pencurian data masih akan menjadi tren di Indonesia pada 2023. Data dalam jumlah massif semakin dibutuhkan oleh banyak pihak, baik untuk kegiatan legal maupun ilegal. Memang ini terjadi secara global, namun dengan pemakai internet hingga tahun ini yang menembus lebih dari 210 juta penduduk, tentunya Indonesia harus lebih serius dalam permasalahan ini.

“Belum lagi masalah kegaduhan yang disebabkan oleh Bjorka yang merupakan sosok yang menghebohkan dunia internet Indonesia dari bulan Agustus dan membuat pemerintah Indonesia ketar ketir. Bjorka adalah hacker yang diduga yang membocorkan dan meretas berbagai institusi pemerintah dan swasta, mulai dari dugaan membocorkan data Indihome, data registrasi SIM CARD, sampai dengan meretas situs Kementerian Komunikasi dan Informatika (Kominfo). Bahkan, Bjorka juga membocorkan data yang dia klaim sebagai data pedulilindungi,” terang Pratama.

Khusus Indonesia karena menjelang pemilu 2024 yang akan terjadi adalah saling retas antar akun media sosial, bahkan bisa merembet saling retas ke website dan

aplikasi milik pemerintah. Ini harus diantisipasi sejak awal.

“Karena itu berbagai kebocoran data masih akan banyak terjadi, akan bertambah parah jika itu juga terjadi karena adanya persaingan politik baik di internal lembaga atau diatasnya. Karena kebocoran data terjadi oleh 3 faktor, yaitu serangan siber, sistem yang eror dan faktor manusia sebagai operatornya,” tegasnya.

Menurut Pratama, saat ini ada beberapa hal yang bisa dilakukan secara umum dalam perbaikan siber, yang pertama dengan mengembangkan prinsip-prinsip inti, standar teknis untuk memastikan tingkat keamanan siber yang konsisten di semua perusahaan yang terlibat. Lalu yang kedua membuat Strategi keamanan siber nasional yang dapat ditindaklanjuti. Ketiga dengan meningkatkan prosedur dan regulasi infrastruktur rantai pasokan. Terakhir ialah dengan melakukan kerjasama Pribadi maupun publik untuk memberikan timbal balik dan kapasitas infrastruktur keamanan siber.

“Kita memang sudah memiliki UU Perlindungan data Pribadi, namun masih belum berlaku efektif. Kita tunggu juga nanti lahirnya Komisi PDP sebagai lembaga yang menjalankan amanat UU PDP. Jadi di 2023 UU PDP ini masih belum bisa berlaku efektif,” tegas Pratama.

Narasumber
Dr. Pratama Persadha
Chairman CISSReC