INDONESIA SATU

# Waspadai Peretasan, ITS Imbau Lindungi Data Pribadi

Achmad Sarjono - SURABAYA.INDONESIASATU.ID

Sep 20, 2022 - 17:25

*Pakar keamanan data dari ITS Bekti Cahyo Hidayanto SSi MKom menghimbau untuk mewaspadai peretasan*

SURABAYA – Belakangan ini, Indonesia dihebohkan perihal peretasan data di beberapa instansi pemerintahan. Akibatnya, berbagai instansi makin gencar untuk meningkatkan keamanan data mereka.

Menanggapi hal tersebut, pakar keamanan data dari Institut Teknologi Sepuluh

Nopember (ITS) Bekti Cahyo Hidayanto SSi MKom mengimbau kepada masyarakat, termasuk sivitas akademika ITS, untuk lebih waspada akan bahaya peretasan data tersebut.

Dosen Departemen Sistem Informasi ITS ini mengungkapkan bahwa serangan siber dapat disebabkan oleh berbagai faktor. Namun, faktor “manusia” yang memiliki akses ke sumber daya Teknologi Informasi (TI) adalah faktor yang paling sulit. Umumnya karena kurangnya pengetahuan tentang keamanan siber, budaya, dan juga kecerobohan.

Orang yang memiliki akses ke aplikasi dan atau sumber data dikelabui dengan tautan phising. “Dengan teknik phising apalagi digabungkan dengan teknik social engineering, cracker memancing korban dengan memberikan tautan untuk menarik data akun yang terdiri dari username dan password,” ungkapnya, Selasa (20/9/2022).

Penggunaan password yang mudah ditebak juga memudahkan cracker untuk melakukan brute force dengan aplikasi. Yakni upaya untuk mengakses sebuah akun dengan cara menebak username dan password. “Tak main-main, mereka bisa membobol dalam hitungan detik dengan algoritma tertentu untuk meretas username dan password para user,” tandas Bekti mengingatkan.

Akibatnya, lanjut Bekti, data bisa disalahgunakan apabila jatuh ke tangan yang salah. Antara lain bisa berupa pembobolan rekening, penipuan, menjatuhkan reputasi, manipulasi data, black campaign, dan lainnya. Setelah berhasil meretas, cracker tidak menghilangkan jejaknya begitu saja. “Biasanya, mereka akan mengarahkan seolah-olah jejaknya ada dan jika diforensik akan menjadikan orang lain sebagai kambing hitam atas perbuatannya,” jelas dosen berkacamata tersebut.

Selain itu, Bekti menuturkan bahwa ada beberapa cara yang bisa dilakukan admin untuk meningkatkan keamanan data, yaitu membuat Disaster Recovery Center dan melakukan Penetration Testing. Disaster recovery adalah membangun server salinan yang menggantikan server utama ketika terjadi masalah. Kemudian, penetration testing adalah tindakan pencegahan secara rutin yang dilakukan untuk mencari celah keamanan pada sistem agar sistem tidak mudah ditembus.

Ilustrasi peretasan data (sumber dari Liputan6.com)

Beralih ke ITS, Bekti menegaskan bahwa ITS memiliki enkripsi data yang baik. Secara infrastruktur, hardware dan software ITS seharusnya sudah tersusun dengan baik sejak sistem dibangun. “Sistem yang baik pun harus didukung juga dengan user yang bijak dalam menjaga data mereka, seperti tidak memberikan username dan password pribadi kepada orang lain,” ujar Bekti.

Selaras dengan hal tersebut, Kepala Unit Komunikasi Publik (UKP) ITS Dr Rahmatsyam Lakoro SSn MT berpesan bahwa keamanan data dapat dilihat dari perspektif teknologi dan sosial. Dari perspektif teknologi, ITS telah berupaya untuk memaksimalkan perlindungan data sivitas akademikanya. “Sedang dari perspektif sosial, keamanan data adalah interaksi sivitas akademika ITS, baik mahasiswa, dosen, maupun tenaga kependidikan terhadap pemanfaatan data tersebut,” tuturnya.

Ia juga menjelaskan, modus social engineering yang marak sebagai bentuk penipuan untuk mengambil data dapat dicegah dengan mengikuti prosedur dan mekanisme pemberian data. “Jangan pernah memberikan data pada pihak yang tidak dikenal. Prosedurnya, akan selalu ada permintaan resmi, bukan hanya melalui pesan langsung misalnya,” tegas dosen Departemen Desain Komunikasi Visual (DKV) ini mengingatkan. (HUMAS ITS)

Reporter: Thariq Agfi Hermawan