

# Pakar IT UGM: Waspadai Serangan Siber di Masa Pandemi

Wednesday, 22 Juli 2020 WIB, Oleh: Gusti



Di masa pandemi sekarang ini, kegiatan pertemuan lewat daring dan perbelanjaan secara online kian marak. Sebab, lewat teknologi komunikasi dan informasi memberikan layanan bagi orang untuk berinteraksi tanpa berhadapan langsung sehingga bisa meminimalkan risiko penularan Covid-19. Namun begitu, sangat disayangkan akhir-akhir ini jutaan data akun pengguna bocor akibat serangan siber sehingga berisiko untuk disalahgunakan.

Pakar bidang teknologi informasi dari Universitas Gadjah Mada, Ir. Lukito Edi Nugroho, M.Sc., Ph.D., mengatakan perlindungan data bagi pemilik akun digital sangat diperlukan. Namun, maraknya serangan siber pada aplikasi belajar daring dan aplikasi e-commerce menunjukkan masih rentannya sistem keamanan yang dimiliki sebuah aplikasi. "Serangan kebanyakan berasal dari luar, tetapi kerentanan bisa muncul dari dalam," kata Lukito kepada wartawan, Rabu (22/7).

Menurut Dosen Teknik Elektro dan Teknologi Informasi, Fakultas Teknik UGM ini serangan siber bisa sering terjadi, tapi kalau sistemnya tangguh maka tidak akan tembus. Sebaliknya, sistem yang rentan dengan banyak celah keamanannya ketika diserang ringan saja bisa bobol. Sementara kerentanan yang disebabkan dari dalam berasal dari kecerobohan penggunaan akun yang tidak diproteksi dengan baik sehingga bisa dibajak orang dan digunakan untuk membobol dari dalam.

Ia menjelaskan bahwa data akun yang bocor tersebut sering untuk diperjualbelikan atau bahkan hanya ajang pamer kemampuan. "Bisa dua-duanya. Kalau datanya bernilai ekonomis misal data pribadi, data kartu kredit, bisa diperjualbelikan," paparnya.

Data akun yang bocor lalu disalahgunakan sehingga bisa mengganggu privasi. Sebab, data akun yg bocor bisa digunakan untuk mendapatkan keuntungan finansial secara tidak sah dan merugikan

pemilik data. Hal itu bisa diketahui dari adanya orang lain yang mengetahui nomor kontak pribadi sambil menawarkan produk. “Tiba-tiba ditelpon oleh orang tidak dikenal, menawari produk ini dan itu. Ada spam telepon. Kasus yg lebih serius, dengan beberapa data tambahan seperti NIP, alamat rumah, nama ibu kandung,” katanya.

Untuk mengurangi dampak dari serangan siber ini, menurutnya yang harus dilakukan adalah hati-hati dalam menyampaikan semua data dalam mendaftarkan akun.” Jika kita tidak percaya dengan aplikasinya, jangan gunakan aplikasi tersebut,” katanya.

Bagi institusi penyelenggara pendidikan yang melaksanakan kegiatan belajar mengajar secara daring, si pemilik akun dan pengelola kegiatan harus melakukan perlindungan akun agar tidak bocor dan disalahgunakan. “Mahasiswa atau siswa sebagai pengguna harus bertanggung jawab terhadap pengamanan akun, aplikasi, dan data yang digunakan. Institusi bertanggung jawab pada sisi infrastruktur termasuk jaringan komputer, server, dan sistem database,” ujarnya.

Soal aturan perlindungan dan keamanan data yang masih minim di Indonesia, Lukito mengusulkan perlu dibuat aturan yang ketat dan penegakan hukum yang lebih tegas sehingga bisa memberikan perlindungan bagi pemilik data. “Memang perlu, tapi yang lebih perlu adalah penegakan hukumnya,” pungkasnya.

Penulis : Gusti Grehenson

Foto : Cyber Attack.msn.com

---

## **Berita Terkait**

- [Insig2 Croatia dan UGM Kerja Sama Pengembangan Keamanan Siber dan Forensik Digital](#)
- [Waspada Serangan Jantung, Kenali Gejalanya](#)
- [CfDS UGM Ungkap Tiga Ancaman Siber Pemilu 2019](#)
- [Kesiapan Keamanan Siber Indonesia di Era Revolusi Industri 4.0](#)
- [RDK UGM 1442H : Refleksi Sinergi Ilmu dan Agama Menghadapi Pandemi](#)