Pusat Penelitian
Badan Keahlian DPR RI
Gd. Nusantara I Lt. 2
Jl. Jend. Gatot Subroto
Jakarta Pusat - 10270
☎ 5715409 🖷 5715245
✉ infosingkat@gmail.com

BIDANG POLITIK DALAM NEGERI
INFO Singkat
KAJIAN SINGKAT TERHADAP ISU AKTUAL DAN STRATEGIS Vol. XIII, No.16/II/Puslit/Agustus/2021

URGENSI PEMBENAHAN SISTEM KEAMANAN SIBER PEMERINTAH

Siti Chaerani Dewanti

Abstrak

Kasus serangan siber yang terjadi pada situs setkab.go.id menambah panjang daftar kasus serangan siber terhadap instansi pemerintah. Hal ini menunjukkan, sistem keamanan siber di Indonesia masih lemah. Tulisan ini membahas ancaman siber di Indonesia serta upaya yang dapat dilakukan untuk meningkatkan keamanan siber. Peningkatan pengguna internet di Indonesia selama masa pandemi dimanfaatkan oleh pelaku kejahatan siber. Badan Siber dan Sandi Negara mencatat adanya peningkatan serangan siber yang sangat signifikan pada periode Januari-November 2020. Upaya yang dapat dilakukan dalam meningkatkan keamanan siber yakni mengubah pola pikir terkait serangan siber, perbaikan sistem informasi dan infrastrukturnya, mempersiapkan sumber daya manusia yang mumpuni, dan memastikan tersedianya regulasi yang mengatur kewajiban pengelola data. Komisi I DPR RI perlu segera menyelesaikan pembahasan Rancangan Undang-Undang Keamanan dan Ketahanan Siber serta Rancangan Undang-Undang Pelindungan Data Pribadi. Selain itu, DPR RI perlu mengevaluasi kinerja mitra kerja yang terkait dengan keamanan siber dan mendorong upaya perbaikan serta kerja sama dari semua pihak.

Pendahuluan

Situs resmi Sekretariat Kabinet Indonesia kembali diretas pada akhir Juli 2021. Akibat dari peretasan tersebut, laman www.setkab.go.id tidak dapat diakses oleh masyarakat. Situs setkab merupakan situs milik pemerintah yang menyajikan berbagai informasi mengenai program dan kinerja pemerintah kepada publik. Namun ketika diretas, situs tersebut hanya menampilkan layar berwarna hitam dengan gambar seorang demonstran dengan tulisan narasi kekecewaan terhadap pemerintah di bawahnya (medcom.id, 11 Agustus 2021).

Kasus serangan siber terhadap situs setkab tersebut menambah panjang kasus peretasan terhadap situs daring instansi pemerintah. Berdasarkan hasil penelusuran pada situs komunitas peretas global, dalam kurun waktu 1 Desember 2020 - 4 Agustus 2021 ditemukan 33.748 kali peretasan terhadap situs berdomain .go.id alias domain

PUSLIT BKD
9 772088 235001

resmi lembaga negara (Kompas, 11 Agustus 2021). Mayoritas peretasan terjadi pada situs resmi instansi di tingkat daerah dari pemerintah, kepolisian, hingga penyelenggara pemilu. Sedangkan di tingkat pusat, terjadi setidaknya 104 peretasan (medcom.id, 10 Agustus 2021).

Meningkatnya implementasi Sistem Pemerintahan Berbasis Elektronik (*e-government*) juga menjadi target para peretas karena menyimpan data pribadi masyarakat luas. Kasus pencurian data pribadi yang terakhir adalah kejadian kebocoran *database* Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan pada Mei 2021. Data yang berisi informasi sensitif tersebut bahkan diperjualbelikan pada forum *online*.

Melihat semakin banyaknya kasus serangan terhadap situs pemerintahan menunjukkan bahwa sistem keamanan siber di Indonesia masih lemah dan belum maksimal. Tulisan ini membahas ancaman siber di Indonesia serta upaya yang dapat dilakukan untuk meningkatkan keamanan siber.

Ancaman Siber di Indonesia

Indonesia merupakan salah satu negara dengan pengguna internet terbesar di dunia. Berdasarkan data *We Are Social* pada awal tahun 2021, jumlah pengguna internet di Indonesia meningkat 15,5%, yang berarti sudah mencapai 202,6 juta jiwa (wearesocial.com, Januari 2021). Hal ini menunjukkan bahwa penetrasi internet di Indonesia mencapai 73,7%. Adanya pandemi covid-19 yang terjadi di seluruh dunia, turut berakibat pada meningkatnya penggunaan internet. Di Indonesia sendiri, durasi penggunaan internet per harinya mencapai 8 jam 52 menit, dan mayoritas pengguna tersebut, sebanyak 96,4%, mengaksesnya dari perangkat *mobile*.

Momentum tingginya penggunaan internet di kala pandemi ini akhirnya juga dimanfaatkan oleh para pelaku kejahatan siber. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa telah terjadi lebih dari 423 juta serangan siber selama periode Januari-November 2020 (cloud.bssn.go.id, 22 Desember 2020). Jumlah tersebut bahkan tiga kali lebih banyak dibandingkan dengan tahun sebelumnya pada periode yang sama yang hanya berjumlah 182 juta.

Menurut *Director of Cyber Security at* BDO Indonesia, Novel Ariyadi, situs pemerintah mudah diretas karena keamanan sistem hanya dijaga seperti penyediaan layanan bagi publik, yakni hanya pada saat jam kerja. Padahal seharusnya kesiapsiagaan atas ancaman siber harus 24 jam. Sedangkan menurut BSSN, tata kelola keamanan siber di instansi pemerintah memang masih sangat kurang. Dari level kematangan skala empat, rata-rata masih berada di level 2-2,5 (Kompas, 12 Agustus 2021).

Gambar 2. Perbandingan Jumlah Serangan Siber di Indonesia
Sumber: BSSN, 2020

Berdasarkan Pedoman Pertahanan Siber tahun 2014, bentuk ancaman siber yang sering terjadi antara lain: a) *Advanced Persistent Threats* (APT), *Denial of Services* (DoS), dan *Distributed Denial of Service* (DDoS), b) *Defacement*, c) *phishing*, d) *malware*, e) *trojan horse,* dan sebagainya. Serangan terhadap situs setkab merupakan serangan *defacement*, yaitu peretas melakukan modifikasi terhadap halaman situs sehingga isi dari halaman web yang dituju berubah sesuai dengan keinginan peretas.

Dalam sistem pemrograman, *deface* website sering dilakukan untuk pengujian awal keamanan karena peretasan dengan teknik tersebut tidak memerlukan keahlian yang tinggi. Hal ini justru menjadi sangat ironis karena menunjukkan bahwa situs-situs lembaga negara dengan mudahnya diserang oleh para peretas pemula. Terbukti bahwa pelaku peretasan situs setkab adalah dua orang pemuda berusia belasan tahun dengan motif menunjukkan jati diri serta mencari keuntungan.

Akibat dari peretasan tersebut adalah terganggunya kelancaran sistem informasi setkab karena tidak dapat diakses untuk beberapa hari. Namun setkab memastikan bahwa tidak ada data rahasia negara yang dicuri karena tidak berisi dokumen rahasia atau yang dikecualikan, melainkan hanya informasi kegiatan presiden dan jajaran menterinya.

Serangan siber lain yang pernah terjadi salah satunya adalah kebocoran data pada sistem *database* BPJS Kesehatan. Akibat dari serangan tersebut, data pribadi milik 279 juta penduduk Indonesia berhasil dicuri dan diperjualbelikan dalam forum *online* (*dark web*). Data yang diperjualbelikan tersebut termasuk di antaranya nama lengkap, NIK, tanggal lahir,

email, hingga nomor ponsel. Adapun data tersebut dijual dengan harga 0,15 bitcoin atau setara dengan sekitar Rp. 81,6 juta (tekno.kompas.com, 22 Mei 2021). Bocornya data tersebut sangat berbahaya karena data kependudukan rentan untuk dieksploitasi. Data tersebut bisa dimanfaatkan untuk kejahatan siber lainnya seperti peretasan akun bank atau penggunaan pinjaman *online* yang tidak bertanggung jawab.

Upaya Peningkatan Keamanan Siber

Pada dasarnya ancaman pada ruang siber bersifat sangat dinamis karena senantiasa *update* dengan perkembangan teknologi. Belum ada satupun teknologi yang dapat menjamin keamanan dari peretasan. Namun, dari berbagai kasus peretasan yang menyerang situs pemerintah, ada beberapa upaya yang dapat dilakukan dalam meningkatkan keamanan siber:

Pertama, perlu adanya perubahan pola pikir bahwa serangan bisa terjadi kapan saja. Ancaman di ruang siber adalah ancaman modern, yang tidak memiliki batas-batas fisik. Ancaman tersebut adalah ancaman aktual yang dapat terekskalasi dari lingkup lokal, nasional, regional, dan internasional. Untuk itu program peningkatan kesadaran (*awareness*) perlu dilakukan di setiap *stakeholders*.

Kedua, perbaikan sistem informasi elektronik dan infrastrukturnya. Pembuatan situs oleh setiap instansi seharusnya bukan semata agar memiliki laman yang bisa diakses masyarakat. Pengelola situs juga perlu memperbarui keamanan sistem secara rutin dan memasang *firewall* serta perangkat pendukung lain. Audit berkala terhadap komponen yang memiliki celah kerentanan harus dilakukan agar tidak dimanfaatkan para peretas. Pengelola sistem informasi juga harus memiliki Pedoman Manajemen Keamanan Informasi yang dapat dijadikan acuan, terutama ketika menghadapi insiden terkait serangan siber.

Ketiga, menyiapkan sumber daya manusia yang mumpuni. Sumber daya manusia yang melaksanakan keamanan siber harus memiliki kompetensi dan senantiasa sigap dalam mengikuti dinamika lingkungan siber yang terus berkembang seiring berkembangnya teknologi dan kondisi sosial masyarakat. BSSN telah mengembangkan jabatan fungsional yang sandiman dan manggala informatika, sebagai jabatan yang bertanggung jawab dalam bidang siber. Diharapkan jabatan tersebut juga dapat dihadirkan pada seluruh instansi sehingga sistem elektronik pemerintah dapat dikawal oleh tenaga yang terdidik dan kompeten.

Keempat, memastikan tersedianya regulasi yang secara komprehensif mengatur tentang keamanan siber, mengingat laju lalu lintas (*traffic*) internet akan semakin tinggi terutama di masa pandemi sekarang ini. Penanganan ancaman serangan siber saat ini masih menggunakan UU Informasi

dan Transaksi Elektronik (UU ITE), yang tercakup di dalamnya untuk beberapa pelanggaran seperti mendistribusikan konten ilegal, pelanggaran pelindungan data, akses tidak berizin ke sistem informasi, hingga penyadapan tidak berizin. Akan tetapi UU ITE ini belum mencakup aspek penting terkait keamanan siber seperti infrastruktur informasi dan jaringan, sumber daya manusia, sistem manajemen, dan sebagainya. Selain itu perlu adanya peraturan yang mengatur kewajiban pengelola data, khususnya yang menyimpan data pribadi, untuk menjaga sistem keamanan sibernya.

Penutup

Semakin maraknya serangan siber terhadap situs milik lembaga negara sudah sepatutnya menjadi pemicu untuk menyadari ancaman siber adalah hal yang perlu diwaspadai sebagai ancaman di era teknologi informasi sekarang ini. Meningkatnya penggunaan situs pemerintah untuk pelayanan terutama sejak masa pandemi ini harus disertai dengan kerja keras dan kesadaran dari setiap instansi dalam pengelolaan sistem informasi dan sistem keamanannya.

Komisi I DPR RI perlu menyelesaikan pembahasan Rancangan Undang-Undang Keamanan dan Ketahanan Siber guna tersedianya peraturan yang secara komprehensif terkait keamanan siber. Rancangan Undang-Undang Pelindungan Data Pribadi juga perlu segera diselesaikan agar tersedianya regulasi yang mengatur kewajiban pengelola data untuk menjaga sistem keamanan sibernya. DPR RI juga perlu mengevaluasi kinerja mitra kerja yang terkait keamanan siber serta mendorong upaya perbaikan dan kerja sama dari semua pihak, karena pada hakikatnya keamanan siber bukan hanya tanggung jawab BSSN, tetapi juga setiap instansi pemerintah.

Referensi

"Audit Berkala Sistem Keamanan Siber", *Kompas*, 12 Agustus 2021, hal. 2.

"Banyak Situs Pemerintahan Rentan Diretas", 10 Agustus 2021, https://video.medcom.id/primetime-news/zNAprBnK-banyak-situs-pemerintahan-rentan-diretas, diakses 14 Agustus 2021.

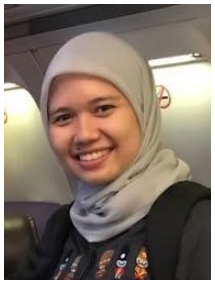
"Digital 2021: Global Overview Report", https://wearesocial.com/digital-2021, diakses 15 Agustus 2021.

"Kronologi Kasus Kebocoran Data WNI, Dijual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS", 22 Mei 2021, https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan?page=all, diakses 15 Agustus 2021.

"Saatnya Perkuat Pengamanan Laman Daring", *Kompas*, 11 Agustus 2021, hal. 2.

"Strategi Keamanan Siber dan Pertumbuhan Ekonomi Digital", Press Release Badan Siber dan Sandi Negara, 22 Desember 2020, https://cloud.bssn.go.id/mE6sEZBW6Ycre#pdfviewer, diakses 15 Agustus 2021.

"8 Fakta Situs Sekretaris Kabinet Diretas Dua Remaja", 11 Agustus 2021, https://www.medcom.id/nasional/peristiwa/Rb1zpddk-8-fakta-situs-sekretaris-kabinet-diretas-dua-remaja, diakses 14 Agustus 2021.



Siti Chaerani Dewanti
siti.dewanti@dpr.go.id

Siti Chaerani Dewanti, menyelesaikan pendidikan S-1 Arsitektur di Fakultas Teknik Universitas Indonesia pada tahun 2009 dan pendidikan S-2 Ilmu Komunikasi di Fakultas Ilmu Sosial Ilmu Politik Universitas Indonesia pada tahun 2014. Saat ini menjabat sebagai Peneliti Pertama Bidang Politik Dalam Negeri untuk kepakaran Komunikasi Media. Kajian-kajian tentang media digital dan media sosial menjadi fokus ilmiahnya. Beberapa tulisan yang telah diterbitkan dalam bagian buku antara lain "Penggunaan Teknologi Informasi dalam Peningkatan Pelayanan Publik di Daerah" (2020), "Penggunaan Website Desa sebagai Media Informasi Desa" (2019) dan "Tata Kelola Website Desa dalam Mewujudkan Transparansi dan Akuntabilitas Dana Desa" (2018).

Info Singkat

http://puslit.dpr.go.id
ISSN 2088-2351