Siaran Pers ELSAM

Mengantisipasi Ancaman dan Risiko Keamanan Siber dalam Pemilu 2024

Perkembangan teknologi informasi dan komunikasi telah mendorong hadirnya sejumlah inovasi dalam penyelenggaraan pemilihan umum (Pemilu). Salah satunya adalah pengembangan berbagai sistem informasi kepemiluan, yang diharapkan dapat memudahkan penyelenggara dalam melakukan pemrosesan data Pemilu, maupun juga memudahkan akses publik untuk mengakses dan mengawasi berbagai data yang diproses dalam penyelenggaraan Pemilu. Seperti halnya Sistem Informasi Pendataan Pemilih (SIDALIH), yang digunakan untuk menyusun, melakukan pemutakhiran dan konsolidasi data pemilih. Namun demikian, inovasi dan efektivitas yang ditawarkan tersebut, juga sekaligus menghadirkan pedang bermata dua, akibatnya besarnya risiko dan ancaman terhadap eksploitasi data Pemilu, khususnya data pribadi pemilih, sebagai akibat kerentanan keamanan sistem informasi yang dikembangkan oleh Komisi Pemilihan Umum (KPU).

Baru-baru ini, pada Senin, 27 November 2023, sebuah akun anonim Jimbo di BreachForum mengunggah 252,327,304 data yang diklaim berasal dari situs kpu.go.id. Data yang dijual seharga $74000 ini paling sedikit terdiri atas NIK, NKK, Nomor KTP, Paspor, nama, tempat pemungutan suara, status difabel, jenis kelamin, tanggal dan tempat lahir, status perkawinan, serta alamat. Merespon hal itu, KPU mengatakan bahwa elemen-elemen data tersebut memang identik dengan data pemilih, oleh karenanya KPU menyebutkan akan melakukan investigasi mendalam atas dugaan insiden kebocoran data itu. Sebelumnya, pada 21 Mei 2020, melalui akun Twitter *underthebreach*, sebuah akun pemantauan dan pencegahan kebocoran data asal Israel, menyebutkan adanya penjualan 2 juta data pemilih yang berasal dari KPU. Penjual juga meyakinkan bahwa dia memiliki 200 juta data penduduk yang terdiri dari nama lengkap, alamat, nomor identitas, tanggal lahir, umur, status kewarganegaraan, dan jenis kelamin. Pada saat itu, KPU menyatakan bahwa data pemilih Pemilu 2014 tersebut masuk dalam kategori data terbuka menurut UU Pemilu.

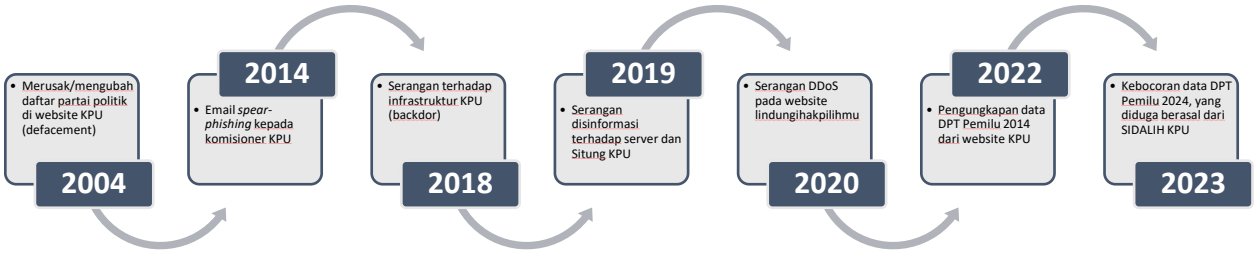
Dari insiden tersebut, mestinya KPU dapat melakukan sejumlah langkah antisipasi, selain memitigasi dan menginvestigasi dugaan insiden kebocoran data yang terjadi, mengingat besar dan sensitifnya data yang dikelola oleh KPU. Dari data pemilih, KPU sedikitnya memproses data: nama, alamat, jenis kelamin, usia, NIK, NKK, paspor, SPLP, tanggal lahir, tempat lahir, status perkawinan, alamat, kondisi disabiltas, dengan total jumlah pemilih mencapai 204.807.222. Sementara data calon meliputi: nama, tempat lahir, tanggal lahir, agama, status perkawinan, alamat, riwayat pendidikan, riwayat pekerjaan, riwayat organisasi, riwayat penghargaan, dan riwayat perjuangan. Kemudian data pengurus Parpol, yang meliputi: nama, NIK, tempat lahir, tanggal lahir, pekerjaan, jenis kelamin, jabatan di Parpol, dan alamat. Sayangnya, dari praktik yang ada justru tidak pernah ada proses investigasi yang tuntas, atas berbagai insiden serangan siber dan dugaan kebocoran data pribadi yang dialami KPU, sehingga tidak ada upaya dan jaminan untuk memastikan ketidakberulangan.

Keseluruhan pemrosesan data yang dilakukan oleh KPU, selain tunduk pada UU Pemilu, dalam konteks pemrosesan data pribadi semestinya juga mengikuti seluruh standar kepatuhan pelindungan data pribadi yang diatur oleh UU No. 27/2022 tentang Pelindungan Data Pribadi. Selain itu sebagai bagian dari penyelenggara sistem elektronik (PSE) lingkup publik, sejumlah persyaratan dalam PP No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) dan Permenkominfo No. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem

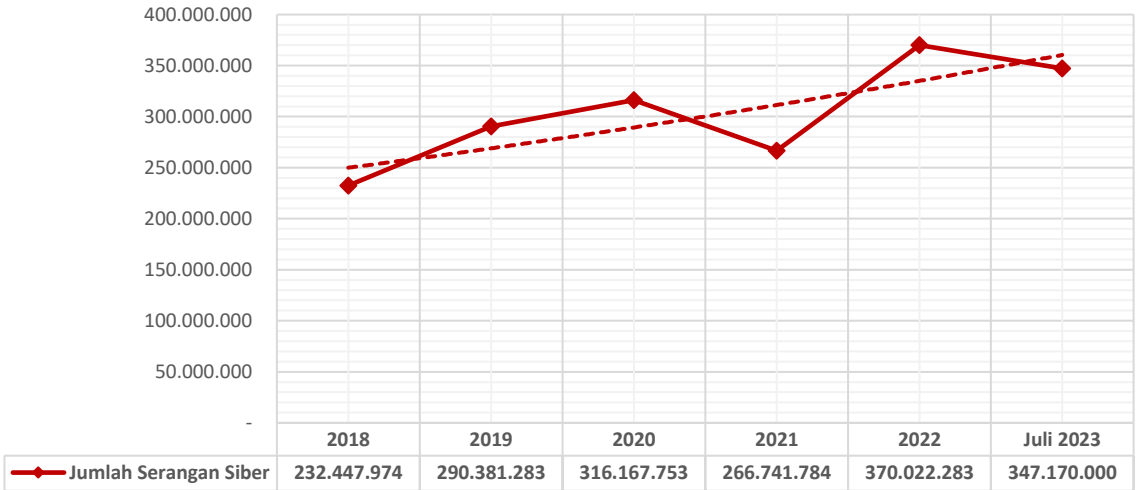
Lembaga Studi dan Advokasi Masyarakat (ELSAM)
Jl. Siaga II No. 31, Pejaten Barat, Pasar Minggu, Jakarta 12510, Indonesia
Telp. (62-21) 797 2662, 7919 2564 Fax. (62-21) 7919 2519
Email : office@elsam.or.id Website : www.elsam.or.id

Elektronik, juga harus diikuti. Dalam hal keamanan sistemnya, sistem informasi yang dikelola KPU, juga tunduk pada Perpres No. 95/2018 tentang Sistem Pemerintahan Berbasis Elektronik (Perpres SPBE), yang secara teknis operasionalnya telah diatur dalam Peraturan BSSN No. 4/2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Peraturan BSSN 4/2021). Dalam peraturan tersebut telah diatur sejumlah syarat dan prosedur keamanan dalam setiap pengembangan sistem informasi yang dilakukan oleh pemerintah, termasuk kewajiban melakukan audit keamanan secara berkala.

Berbagai Bentuk Serangan Siber Terhadap KPU



Langkah-langkah tersebut penting dilakukan, sebagai bagian dari manajemen risiko keamanan siber, yang meliputi kepatuhan terhadap peraturan perundang-undangan, kesesuaian dengan standar yang berlaku, dan sistem pengendalian internal (Perpres No. 82/2022). Apalagi mengingat besarnya ancaman dan risiko serangan siber terhadap sistem informasi pemerintah, sebagaimana dikemukakan oleh Badan Siber dan Sandi Negara (BSSN). Dari catatan BSSN juga tampak, adanya peningkatan masif serangan siber ke Indonesia, pada saat penyelenggaraan Pemilu, seperti yang terjadi di tahun 2019. Hal ini juga bisa kita lihat dari tren kenaikan serangan siber ke Indonesia dalam lima tahun terakhir:



	2018	2019	2020	2021	2022	Juli 2023
Jumlah Serangan Siber	232.447.974	290.381.283	316.167.753	266.741.784	370.022.283	347.170.000

Sumber: https://honeynet.bssn.go.id/, 2023.

Lembaga Studi dan Advokasi Masyarakat (ELSAM)
Jl. Siaga II No. 31, Pejaten Barat, Pasar Minggu, Jakarta 12510, Indonesia
Telp. (62-21) 797 2662, 7919 2564 Fax. (62-21) 7919 2519
Email : office@elsam.or.id Website : www.elsam.or.id

Data tersebut menunjukkan tren kenaikan dari 2018 ke 2019 (pada saat berlangsung Pemilu 2019), dan meningkat kembali pada 2020, sebagai akibat dari pandemi COVID-19, ketika banyak orang mengubah metode kerja dari *offline* ke *online*. Data terakhir sampai dengan semester pertama 2023, insiden serangan siber ke Indonesia mencapai 347.170.000 serangan. Diakui BSSN serangan paling banyak dialami oleh sistem informasi pemerintah dan sistem keuangan, dengan bentuk serangan yang beragam, seperti *malware*, *defacement*, dan sebagian lagi *hacking* yang berdampak pada pengungkapan data pribadi.

Bentuk ancaman dan risiko keamanan siber terhadap keamanan sistem informasi dalam penyelenggaraan Pemilu 2024 juga beragam, baik dalam bentuk *passive attack*, *active attack*, maupun *syntactic* dan *semantic attack*.

Ancaman dan Risiko Serangan Siber dalam Pemilu 2024

Passive Attack	**Active Attack**	**Syntactic and Semantic Attack**
• Computer and network surveillance • Network - Wiretapping - Fiber tapping - Port scan - Idle scan • Host - Keystroke logging - Data scraping - Backdoor	• Denial-of-service attack • Spoofing • Mixed threat attack • Network - Man-in-the-middle - Man-in-the-browser - ARP poisoning - Ping flood - Ping of death - Smurf attack • Host - Buffer overflow - Heap overflow - Stack overflow - Format string attack	• Syntactic Attacks - Viruses - Worms - Trojan horses - Malware - Ransomware • Semantic Attacks - Modifikasi dan penyebaran informasi yang benar dan salah (disinformasi)

Berbagai ancaman dan risiko tersebut tentunya akan berdampak serius pada proses dan integritas hasil Pemilu 2024, termasuk: permasalahan ketidakpercayaan pada penyelenggara Pemilu, khususnya KPU, yang dianggap tidak mampu untuk menyiapkan sistem informasi yang andal, termasuk upaya untuk meminimalisir dan memitigasi setiap risiko keamanan; potensi naiknya angka Golput, karena kekhawatiran terjadinya eksploitasi data Pemilu, sehingga publik enggan ikut Pemilu; tingkat kepercayaan publik pada hasil Pemilu, terutama terkait dengan integritas data Pemilu, khususnya yang menyangkut pemrosesan data pribadi pemilih maupun calon, termasuk hasil penghitungan dari pemungutan suara; budaya mengabaikan risiko keamanan dan perlindungan data pribadi dalam Pemilu dari penyelenggara pemilu, ketika mereka mengabaikan setiap risiko dan ancaman keamanan sistem yang terkait penyelenggaraan Pemilu; dan dampak bahaya yang melebihi tujuan politik elektoral, akibat serangan keamanan siber dan eksploitasi data pribadi pemilih.

Merespons hal itu, sebagai langkah antisipasi risiko dan ancaman keamanan siber dalam penyelenggaraan Pemilu 2024, penting bagi KPU untuk melakukan sejumlah langkah berikut ini:

- Melakukan asesmen dan audit keamanan terhadap seluruh sistem informasi yang dikembangkan dan dikelola oleh KPU, setidaknya mengacu pada *information technology and security assessment* (ITSA) yang disiapkan oleh BSSN, dengan merujuk pada standar erpres No. 95/2018 dan Per-BSSN No. 4/2021.
- Penyusunan kebijakan perlindungan data pribadi (*privacy policy*), yang menjelaskan keseluruhan proses pelindungan data pribadi, termasuk sistem keamanan yang diterapkan, dengan mengacu pada rangkaian kewajiban pengendali data yang diatur oleh UU PDP, termasuk langkah dan prosedur ketika terjadi pelanggaran.
- Penyusunan pedoman perilaku (*code of conduct*) perlindungan data pribadi dalam penyelenggaraan pemilu, yang menjadi acuan bagi seluruh penyelenggara pemilu.
- Penunjukan petugas/pejabat pelindungan data pribadi, untuk memastikan pemenuhan hak subjek data, termasuk juga penguatan *Computer Security Incident Response Team* (CSIRT), untuk memberikan respons cepat setiap kali terjadi insiden keamanan (siber)
- Penerapan *privacy by design* dan *privacy by default* untuk seluruh sistem informasi elektronik yang dikembangkan, sebagai langkah pencegahan atas terjadinya insiden keamanan.
- Melakukan penilaian dampak pelindungan data pribadi (DPIA) dari seluruh tahapan Pemilu, termasuk terhadap seluruh sistem informasi yang dikembangkan oleh KPU.
- Penyusunan regulasi terkait dengan data akses dan *data sharing* untuk data-data Pemilu dengan pemangku kepentingan, khususnya data yang mengandung konten data pribadi.
- Peningkatan kapasitas bagi seluruh penyelenggara pemilu terkait dengan risiko dan antisipasi keamanan siber dari sistem informasi yang dikelola dan digunakan KPU, termasuk yang terkait dengan pelindungan data pribadi.
- Koordinasi dan kerja sama dengan berbagai pemangku kepentingan terkait, untuk mengoptimalkan langkah-langkah antisipasi dan mitigasi risiko dan insiden keamanan yang mungkin terjadi, dengan tetap menjunjung tinggi prinsip dasar penyelenggaraan Pemilu, langsung, umum, bebas, rahasia, jujur, dan adil.

Lembaga Studi dan Advokasi Masyarakat (ELSAM)

Untuk informasi lebih lanjut silahkan menghubungi: Wahyudi Djafar (Direktur Eksekutif ELSAM), telepon: 081382083993, atau Parasurama Pamungkas (Peneliti ELSAM), telepon: 082232001783, atau Annisa N. Hayati (Peneliti ELSAM), telepon: 081344426673.