NEWS

Dr. Hendri: Keamanan Siber Harus Menjadi Prioritas Pembangunan

Updates. - TNIAD.NET

Jul 18, 2026 - 03:00

Dr. Ir. Hendri, ST., MT Wartawan Utama Ketua Umum Jurnalis Nasional Indonesia (JNI)

OPINI - Indonesia sedang berlomba membangun jalan tol, pelabuhan, pembangkit listrik, pusat data, jaringan telekomunikasi, layanan pemerintahan digital, sistem pembayaran, dan berbagai aplikasi pelayanan publik. Kita ingin menjadi negara maju dengan ekonomi digital yang kuat, birokrasi yang cepat, serta pelayanan yang dapat diakses masyarakat dari mana saja.

Namun, ada satu pertanyaan mendasar yang sering datang terlambat: apakah seluruh sistem tersebut benar-benar aman?

Kita tidak akan membangun bendungan tanpa memperhitungkan kekuatan konstruksinya. Kita tidak akan mengoperasikan bandara tanpa sistem keamanan, pengendalian lalu lintas, dan prosedur keadaan darurat. Kita juga tidak akan membuka rumah sakit tanpa cadangan listrik serta perlindungan terhadap keselamatan pasien.

Anehnya, dalam pembangunan digital, keamanan masih sering diperlakukan sebagai fitur tambahan. Sistem dibuat terlebih dahulu, diluncurkan secepat mungkin, dipromosikan sebagai inovasi, kemudian pengamanan baru dibicarakan setelah terjadi kebocoran data, peretasan, penipuan, atau lumpuhnya pelayanan.

Cara berpikir tersebut harus dihentikan.

Keamanan siber bukan pelengkap transformasi digital. Ia merupakan fondasi pembangunan modern. Tanpa keamanan siber, digitalisasi hanya akan memperluas permukaan serangan, memperbesar risiko, dan memindahkan kelemahan birokrasi dari ruang fisik ke ruang digital.

Pembangunan Kini Bergantung pada Sistem Digital

Hampir seluruh sektor pembangunan saat ini menggunakan sistem elektronik. Data kependudukan, perpajakan, kesehatan, pendidikan, perbankan, bantuan sosial, pertanahan, perdagangan, logistik, energi, transportasi, pertahanan, dan pelayanan administrasi disimpan serta diproses melalui jaringan digital.

Ketika sistem tersebut berjalan baik, pelayanan menjadi lebih cepat, murah, dan mudah diakses. Namun, ketika mengalami gangguan, akibatnya dapat merambat ke berbagai sektor.

Serangan terhadap rumah sakit dapat menghambat penanganan pasien. Gangguan pada sistem pembayaran dapat menghentikan transaksi. Serangan terhadap pembangkit atau distribusi energi dapat memengaruhi kegiatan ekonomi. Kebocoran data kependudukan dapat digunakan untuk penipuan, pinjaman ilegal, pembajakan akun, dan pemalsuan identitas.

Serangan terhadap sistem pemerintahan juga dapat menghentikan layanan imigrasi, perizinan, bantuan sosial, pengadaan, atau pencatatan administrasi. Sementara itu, peretasan media dan akun resmi dapat digunakan untuk menyebarkan informasi palsu seolah-olah berasal dari sumber yang sah.

Artinya, ancaman siber tidak lagi berhenti di dalam komputer. Dampaknya hadir dalam kehidupan nyata: pelayanan terganggu, transaksi terhenti, uang hilang, identitas disalahgunakan, reputasi runtuh, dan kepercayaan masyarakat menurun.

Karena itulah keamanan siber harus dimasukkan sejak tahap perencanaan pembangunan. Setiap proyek digital harus memiliki analisis risiko, desain

keamanan, anggaran pemeliharaan, rencana cadangan, mekanisme pemulihan, serta penanggung jawab yang jelas.

Ancaman yang Terus Membesar

Berdasarkan data BSSN yang disampaikan pemerintah pada Juni 2026, terdapat sekitar 5,5 miliar aktivitas serangan atau anomali siber yang terdeteksi sepanjang 2025. Pada periode 1 Januari hingga 15 April 2026, terdeteksi sekitar 1,52 miliar aktivitas serupa. Kantor Staf Presiden melalui ANTARA

Angka tersebut tidak boleh langsung dimaknai sebagai jumlah kebocoran atau peretasan yang berhasil. Satu aktivitas serangan dapat menghasilkan banyak catatan teknis dan sebagian dapat diblokir oleh sistem. Namun, besarnya volume deteksi tetap memperlihatkan betapa luas dan terus-menerusnya ancaman yang harus dihadapi.

Ancaman tidak hanya berasal dari peretas individual. Pelakunya dapat berupa kelompok kriminal, sindikat penipuan, kelompok pemeras ransomware, aktor negara, kelompok politik, orang dalam, atau penyedia pihak ketiga yang sistemnya berhasil disusupi.

Motifnya juga beragam. Ada yang mencari uang, mencuri data, melakukan pemerasan, memata-matai, mengganggu pelayanan, merusak reputasi, memengaruhi opini publik, atau melemahkan infrastruktur strategis suatu negara.

Kecerdasan buatan membuat ancaman semakin kompleks. Penjahat dapat membuat pesan penipuan yang lebih meyakinkan, meniru suara pimpinan, menghasilkan video palsu, mengotomatisasi pencarian kerentanan, serta melakukan rekayasa sosial dalam skala besar.

Di sisi lain, penggunaan komputasi awan, perangkat Internet of Things, sistem kerja jarak jauh, aplikasi seluler, kecerdasan buatan, dan integrasi antarlembaga terus menambah titik yang harus diamankan.

Semakin terhubung sebuah negara, semakin besar manfaat yang diperoleh. Namun, semakin besar pula akibatnya jika konektivitas itu tidak dibangun dengan aman.

Pelajaran dari Serangan PDNS

Serangan ransomware terhadap Pusat Data Nasional Sementara 2 pada Juni 2024 menjadi peringatan keras. Serangan tersebut berdampak pada sejumlah layanan publik dan memaksa pemerintah melakukan pemulihan secara bertahap. Pemerintah mengakui peristiwa itu sebagai pelajaran penting untuk memperkuat transformasi digital yang lebih aman. Kementerian Komunikasi dan Digital

Pelajaran utamanya bukan hanya bahwa ransomware berbahaya. Peristiwa tersebut menunjukkan keamanan siber merupakan persoalan tata kelola.

Sebuah sistem dapat menggunakan perangkat mahal, pusat data modern, dan jaringan berkapasitas besar. Namun, semuanya tetap rentan apabila inventaris

aset tidak lengkap, akses tidak dibatasi, perangkat lunak tidak diperbarui, pencadangan tidak diuji, tanggung jawab tidak jelas, serta prosedur tanggap insiden tidak pernah dilatih.

Setelah insiden tersebut, pemerintah menyampaikan penguatan berupa autentikasi multifaktor, pembatasan hak akses, prinsip *zero trust*, dan peningkatan tata kelola dari hulu sampai hilir. Kementerian Komunikasi dan Digital

Langkah itu perlu diterapkan secara konsisten ke seluruh kementerian, lembaga, pemerintah daerah, BUMN, fasilitas pelayanan publik, dan mitra penyedia teknologi.

Jangan sampai pembenahan hanya dilakukan ketika perhatian publik sedang tinggi, kemudian kedisiplinan menurun setelah keadaan dianggap normal.

Keamanan Siber adalah Persoalan Tata Kelola

Banyak orang masih menganggap keamanan siber sebagai urusan bagian teknologi informasi. Ketika terjadi insiden, petugas teknis menjadi pihak pertama yang disalahkan. Padahal, keputusan penting mengenai anggaran, pengadaan, jumlah pegawai, standar pelayanan, penyimpanan data, pemilihan penyedia, dan pengelolaan risiko berada pada tingkat pimpinan.

Keamanan siber harus menjadi tanggung jawab pimpinan organisasi.

Menteri, kepala lembaga, gubernur, bupati, wali kota, direktur utama, rektor, kepala rumah sakit, serta pimpinan organisasi harus memahami aset digital yang mereka kelola, risiko yang dihadapi, kemampuan pemulihan, dan konsekuensi hukum apabila data masyarakat tidak terlindungi.

Setiap organisasi setidaknya harus mampu menjawab pertanyaan berikut: data apa yang dimiliki, di mana data disimpan, siapa yang dapat mengakses, perangkat apa yang terhubung, kapan terakhir diperbarui, apakah cadangannya tersedia, berapa lama pelayanan dapat dipulihkan, dan siapa yang mengambil keputusan ketika terjadi krisis?

Jika pertanyaan sederhana tersebut tidak dapat dijawab, organisasi sebenarnya belum memahami risiko digitalnya sendiri.

Kegagalan keamanan sering bukan disebabkan teknologi yang terlalu canggih bagi penyerang, melainkan kelalaian dasar: kata sandi lemah, akun lama yang belum ditutup, perangkat lunak tidak diperbarui, data disalin tanpa izin, akses diberikan terlalu luas, atau pegawai mengklik tautan berbahaya.

Kementerian Komunikasi dan Digital pada Desember 2025 juga menegaskan bahwa kesalahan manusia masih menjadi salah satu faktor risiko utama sehingga pengetahuan keamanan siber harus diperlakukan sebagai keterampilan hidup. Kementerian Komunikasi dan Digital

Keamanan Harus Dibangun Sejak Awal

Pemerintah dan dunia usaha perlu menerapkan prinsip *security by design* dan *privacy by design*. Keamanan serta pelindungan privasi harus masuk sejak sistem dirancang, bukan ditambahkan setelah aplikasi selesai.

Setiap pengembangan sistem perlu dimulai dengan pemetaan kebutuhan dan risiko. Organisasi harus menentukan data apa yang benar-benar diperlukan. Pengumpulan data berlebihan hanya memperbesar risiko apabila terjadi kebocoran.

Data juga harus diklasifikasikan. Informasi yang terbuka untuk publik tentu membutuhkan perlakuan berbeda dari data pribadi, data kesehatan, informasi pertahanan, rahasia dagang, atau kredensial akses.

Hak pengguna harus diberikan berdasarkan kebutuhan kerja minimum. Seorang pegawai tidak perlu memperoleh akses ke seluruh sistem hanya karena bekerja di satu instansi. Ketika berpindah tugas atau berhenti, aksesnya harus segera diperbarui atau dicabut.

Autentikasi multifaktor perlu diwajibkan untuk akun penting. Data sensitif harus dienkripsi ketika disimpan maupun dikirim. Kunci enkripsi tidak boleh disimpan bersama data yang dilindunginya. Sistem harus diperbarui secara berkala, sedangkan kerentanan kritis harus segera ditangani.

Aplikasi juga harus diuji sebelum digunakan. Pengujian tidak cukup hanya memastikan fungsi aplikasi berjalan. Pemerintah perlu melakukan pengujian keamanan, penilaian kerentanan, simulasi serangan, dan pemeriksaan terhadap kode maupun komponen pihak ketiga.

Setelah diluncurkan, sistem harus terus dipantau. Keamanan bukan keadaan yang dicapai sekali, melainkan proses yang harus dipelihara sepanjang umur sistem.

Cadangan Data Harus Benar-Benar Dapat Dipulihkan

Banyak organisasi merasa aman karena memiliki cadangan data. Namun, cadangan yang tersambung terus-menerus dengan sistem utama dapat ikut dienkripsi oleh ransomware. Cadangan yang tidak pernah diuji juga belum tentu dapat digunakan ketika dibutuhkan.

Karena itu, setiap instansi harus memiliki beberapa salinan data, menggunakan media dan lokasi berbeda, serta menyediakan cadangan yang terpisah atau tidak dapat diubah oleh penyerang. Data paling penting perlu disimpan pada wilayah pemulihan bencana yang secara teknis tidak bergantung pada satu pusat data.

Yang lebih penting, organisasi harus menguji proses pemulihan secara berkala.

Keberhasilan pencadangan tidak diukur dari pesan bahwa proses salin telah selesai. Keberhasilan baru terbukti ketika organisasi dapat memulihkan data dan menjalankan pelayanan kembali dalam batas waktu yang telah ditetapkan.

Latihan pemulihan harus melibatkan pimpinan, petugas teknologi, bagian hukum, komunikasi publik, penyedia layanan, dan unit pelayanan. Dalam keadaan krisis, persoalannya bukan hanya memperbaiki server, tetapi juga menentukan prioritas pelayanan, memberi informasi kepada masyarakat, melindungi bukti digital, dan mengambil keputusan operasional.

Lindungi Infrastruktur Informasi Vital

Indonesia telah memiliki Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. Regulasi ini mencakup identifikasi, pelindungan, pembinaan, pengawasan, dan koordinasi terhadap sistem elektronik yang apabila terganggu dapat menimbulkan dampak serius bagi pelayanan publik, pertahanan, keamanan, atau perekonomian nasional. Database Peraturan BPK

Sistem administrasi pemerintahan, energi, keuangan, kesehatan, transportasi, telekomunikasi, pangan, dan sektor strategis lainnya membutuhkan tingkat perlindungan yang lebih tinggi.

Pengelola infrastruktur vital tidak cukup hanya memenuhi dokumen kepatuhan. Mereka harus memiliki pusat operasi keamanan, tim tanggap insiden, pemantauan berkelanjutan, segmentasi jaringan, perlindungan perangkat operasional, cadangan, latihan krisis, dan koordinasi dengan BSSN serta otoritas sektoral.

Rantai pasok juga harus diperiksa. Sistem yang kuat dapat ditembus melalui penyedia perangkat lunak, perusahaan pemeliharaan, konsultan, mitra logistik, atau akun vendor. Setiap pihak yang memperoleh akses harus memenuhi standar keamanan yang sama.

Pemerintah juga perlu menghindari ketergantungan berlebihan pada satu penyedia, satu pusat data, satu jaringan, atau satu teknologi. Sentralisasi dapat meningkatkan efisiensi, tetapi juga menciptakan satu titik kegagalan yang dampaknya sangat luas.

Integrasi harus berjalan bersama segmentasi, redundansi, dan kemampuan pemulihan.

Data Pribadi adalah Hak Warga Negara

Keamanan siber tidak hanya berkaitan dengan rahasia negara. Ia juga melindungi hak warga atas data pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur hak subjek data, kewajiban pengendali dan prosesor data, pemrosesan, transfer, sanksi, serta kelembagaan. Undang-undang tersebut menegaskan bahwa pelindungan data pribadi merupakan bagian dari perlindungan hak konstitusional. Database Peraturan BPK

Setiap lembaga yang meminta masyarakat menyerahkan NIK, alamat, data

biometrik, informasi kesehatan, data keuangan, atau data anak memiliki kewajiban untuk menjaganya.

Masyarakat tidak berada dalam posisi yang setara dengan penyelenggara sistem. Warga sering harus menyerahkan data agar dapat memperoleh layanan. Karena itu, persetujuan tidak boleh dijadikan alasan untuk melepaskan tanggung jawab pengelola.

Negara perlu segera memastikan otoritas pengawas pelindungan data pribadi dapat bekerja secara kuat, profesional, dan independen. Pengawasan tidak boleh hanya bergantung pada laporan sukarela dari lembaga yang mengalami insiden.

Setiap kebocoran harus ditangani melalui investigasi, notifikasi yang jujur, mitigasi bagi korban, perbaikan sistem, dan penegakan sanksi apabila ditemukan kelalaian.

Menutupi insiden demi menjaga citra justru memperbesar kerugian. Korban kehilangan kesempatan mengganti kata sandi, memblokir akun, atau melindungi diri dari penyalahgunaan identitas.

Anggaran Siber adalah Investasi Pembangunan

Keamanan siber sering dianggap sebagai pusat biaya karena tidak secara langsung menghasilkan pendapatan atau pelayanan baru. Pandangan ini keliru.

Fungsi utama keamanan memang mencegah sesuatu terjadi. Keberhasilannya justru sering tidak terlihat. Namun, ketika perlindungan gagal, biaya pemulihan dapat jauh lebih besar daripada investasi pencegahan.

Kerugian tidak hanya berupa uang tebusan atau biaya perbaikan. Organisasi dapat kehilangan data, pendapatan, waktu kerja, kepercayaan masyarakat, peluang investasi, serta kemampuan memberikan pelayanan.

Karena itu, setiap proyek digital harus menyediakan anggaran keamanan sepanjang siklus hidupnya. Biaya tidak berhenti setelah perangkat atau aplikasi dibeli. Diperlukan pembaruan, pemantauan, audit, pelatihan, lisensi, pengujian, pencadangan, dan penggantian teknologi yang sudah tidak didukung.

Pengadaan pemerintah juga harus berubah. Pemenang tidak boleh hanya ditentukan berdasarkan harga termurah. Pemerintah perlu menilai keamanan desain, riwayat kerentanan, dukungan pembaruan, lokasi serta pengelolaan data, kemampuan audit, portabilitas data, rencana penghentian layanan, dan tanggung jawab ketika terjadi insiden.

Kontrak harus mengatur kewajiban pelaporan insiden, waktu perbaikan, pengujian, akses audit, perlindungan data, dan penghapusan data setelah kerja sama berakhir.

Murah pada saat dibeli belum tentu murah ketika sistem mengalami serangan.

Bangun Talenta dan Industri Keamanan Siber

Nasional

Indonesia membutuhkan tenaga keamanan siber dalam jumlah besar: analis, auditor, arsitek keamanan, penguji penetrasi, ahli forensik digital, kriptografer, pengembang perangkat lunak aman, analis malware, ahli hukum teknologi, dan manajer risiko.

Kebutuhan tersebut tidak dapat dipenuhi hanya melalui pelatihan singkat. Pendidikan keamanan siber harus dibangun berjenjang dari sekolah, SMK, perguruan tinggi, lembaga sertifikasi, hingga pelatihan profesional.

Pelajar perlu memahami keamanan digital dasar. Mahasiswa membutuhkan laboratorium, kompetisi, penelitian, magang, dan pengalaman menangani persoalan nyata. ASN serta pegawai swasta harus mendapatkan pelatihan sesuai perannya. Pimpinan organisasi membutuhkan pelatihan manajemen risiko dan pengambilan keputusan ketika terjadi krisis.

Pemerintah juga harus mampu mempertahankan tenaga ahli. Negara tidak dapat melindungi sistem strategis jika tenaga terbaik terus meninggalkan sektor publik karena jenjang karier, lingkungan kerja, dan penghargaan profesional tidak memadai.

Industri keamanan siber nasional perlu diperkuat melalui riset, pengadaan, standardisasi, pengujian, pembiayaan, dan akses pasar. Indonesia harus mampu mengembangkan teknologi enkripsi, identitas digital, deteksi ancaman, forensik, keamanan aplikasi, serta perangkat perlindungan jaringan.

Namun, produk dalam negeri tidak boleh otomatis dianggap aman hanya karena dibuat di Indonesia. Semua produk harus melalui pengujian independen dan memenuhi standar yang dapat dipertanggungjawabkan. Kedaulatan teknologi harus dibangun melalui kemampuan dan mutu, bukan slogan.

Pemerintah Daerah dan UMKM Tidak Boleh Ditinggalkan

Keamanan siber tidak boleh hanya kuat di kementerian pusat, bank besar, dan perusahaan teknologi. Pemerintah daerah, sekolah, rumah sakit daerah, pemerintah desa, koperasi, media lokal, dan UMKM juga mengelola data serta pelayanan penting.

Banyak organisasi kecil menggunakan perangkat lama, aplikasi yang tidak diperbarui, kata sandi bersama, jaringan tanpa segmentasi, dan tenaga teknologi yang terbatas. Kondisi tersebut menjadikannya sasaran yang relatif mudah.

Pemerintah pusat perlu menyediakan standar minimum, layanan keamanan bersama, pendampingan, pusat operasi regional, pelatihan, serta mekanisme tanggap insiden yang dapat diakses daerah.

BSSN telah mengatur penilaian mandiri keamanan informasi bagi UMKM melalui Peraturan BSSN Nomor 4 Tahun 2024. Program semacam ini perlu diperluas dengan bantuan praktis agar UMKM dapat memperbaiki kelemahan yang

ditemukan, bukan sekadar mengisi daftar pemeriksaan. Database Peraturan BPK

UMKM harus dibantu menerapkan pencadangan, autentikasi multifaktor, perlindungan transaksi, pembaruan perangkat, dan pelatihan pegawai. Satu serangan dapat menghabiskan seluruh modal dan menghancurkan kepercayaan pelanggan yang dibangun selama bertahun-tahun.

Media Juga Menjadi Infrastruktur Kepercayaan

Media dan jurnalis memiliki posisi khusus dalam keamanan siber. Akun media yang diretas dapat digunakan untuk menyebarkan berita palsu kepada jutaan orang. Arsip berita dapat dihapus atau diubah. Identitas narasumber dapat terbuka. Komunikasi wartawan dapat dipantau, sedangkan dokumen investigasi dapat dicuri.

Dalam era perang informasi dan kecerdasan buatan, keamanan redaksi merupakan bagian dari perlindungan demokrasi.

Perusahaan media perlu melindungi sistem penerbitan, akun wartawan, arsip, surel, sumber rahasia, dan infrastruktur distribusi. Autentikasi multifaktor, pengelolaan akses, tanda tangan digital, pencadangan arsip, serta prosedur verifikasi konten harus menjadi standar.

Media juga bertanggung jawab meningkatkan literasi masyarakat. Peliputan insiden siber harus akurat dan tidak memperbesar kepanikan. Informasi teknis yang dapat membantu penyerang tidak boleh diumumkan secara sembarangan. Namun, kepentingan keamanan juga tidak boleh dijadikan alasan untuk menutupi kelalaian lembaga publik.

Keamanan Tidak Boleh Menjadi Alasan Pengawasan Berlebihan

Ada kekhawatiran bahwa kebijakan keamanan siber dapat digunakan untuk memperluas pengawasan, membatasi kebebasan berekspresi, atau mengendalikan informasi.

Kekhawatiran tersebut harus dijawab dengan batas hukum yang tegas.

Keamanan siber bertujuan melindungi sistem, data, dan masyarakat dari serangan. Ia tidak boleh menjadi alasan untuk memantau warga tanpa dasar hukum, mengumpulkan data secara berlebihan, atau membungkam kritik.

Setiap kewenangan akses, pemantauan, intersepsi, dan pemrosesan data harus memiliki tujuan yang sah, dasar hukum, batas waktu, pengawasan, serta mekanisme pertanggungjawaban.

Keamanan dan kebebasan bukan dua hal yang harus saling menghilangkan. Ruang digital yang aman justru dibutuhkan agar warga dapat berkomunikasi, bekerja, berusaha, dan menyampaikan pendapat tanpa takut menjadi korban kejahatan maupun penyalahgunaan kekuasaan.

Ukur Keamanan dari Kemampuan Bertahan dan Pulih

Keberhasilan keamanan siber tidak boleh diukur hanya dari jumlah perangkat yang dibeli, aplikasi yang dipasang, rapat yang diselenggarakan, atau tim tanggap insiden yang dibentuk.

Ukuran yang lebih bermakna adalah kemampuan organisasi mengetahui asetnya, menemukan serangan, membatasi dampak, memulihkan pelayanan, melindungi korban, dan mencegah kejadian berulang.

Pemerintah perlu mengukur waktu rata-rata mendeteksi insiden, waktu merespons, waktu memulihkan pelayanan, tingkat keberhasilan pengujian cadangan, jumlah kerentanan kritis yang belum ditangani, kepatuhan autentikasi multifaktor, kualitas pengelolaan akses, serta kesiapan pemasok.

Hasil audit keamanan pada sistem strategis tidak harus dibuka seluruhnya karena dapat mengandung informasi sensitif. Namun, tingkat kepatuhan, status tindak lanjut, kejadian material, dan pertanggungjawaban pimpinan harus dapat diketahui publik.

Transparansi yang tepat akan meningkatkan kepercayaan sekaligus mendorong perbaikan.

Sepuluh Agenda Prioritas

Agar keamanan siber benar-benar menjadi bagian dari pembangunan, Indonesia perlu menjalankan sedikitnya sepuluh agenda.

Pertama, wajibkan analisis risiko dan desain keamanan pada setiap proyek digital yang dibiayai APBN, APBD, atau dana publik lainnya.

Kedua, tetapkan standar minimum keamanan bagi kementerian, lembaga, pemerintah daerah, BUMN, fasilitas publik, dan penyelenggara infrastruktur informasi vital.

Ketiga, wajibkan autentikasi multifaktor, enkripsi, pengelolaan akses minimum, pembaruan sistem, dan segmentasi jaringan pada sistem penting.

Keempat, bangun pencadangan terpisah serta lakukan latihan pemulihan secara berkala.

Kelima, perkuat pusat operasi keamanan dan tim tanggap insiden di tingkat nasional, sektoral, daerah, dan organisasi.

Keenam, percepat penguatan kelembagaan pelindungan data pribadi serta penegakan kewajiban pengendali data.

Ketujuh, reformasi pengadaan teknologi agar keamanan, dukungan pembaruan, dan risiko pemasok menjadi bagian utama penilaian.

Kedelapan, bangun talenta serta industri keamanan siber nasional melalui pendidikan, penelitian, sertifikasi, dan kepastian pasar.

Kesembilan, kembangkan budaya pelaporan insiden yang cepat, jujur, dan tidak menghukum pihak yang melapor dengan itikad baik.

Kesepuluh, lakukan latihan krisis nasional secara rutin dengan melibatkan pemerintah, dunia usaha, perguruan tinggi, media, dan masyarakat.

Keamanan sebagai Syarat Kemajuan

Indonesia sebenarnya telah memiliki arah kebijakan melalui Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Strategi tersebut kemudian dijabarkan melalui Rencana Aksi Nasional Keamanan Siber 2024–2028. Database Peraturan BPK

Kerangka regulasi telah tersedia. Yang menentukan adalah pelaksanaannya.

Keamanan siber harus masuk ke dalam perencanaan pembangunan, penganggaran, pengadaan, penilaian kinerja, pendidikan, dan pertanggungjawaban pimpinan. Ia tidak boleh hanya menjadi urusan petugas teknis atau dibicarakan setelah insiden terjadi.

Transformasi digital yang tidak aman akan mengubah efisiensi menjadi kerentanan, integrasi menjadi perluasan dampak, dan data menjadi alat kejahatan. Sebaliknya, keamanan yang kuat akan membangun kepercayaan, memperlancar investasi, menjaga pelayanan, serta memperkokoh kedaulatan negara.

Indonesia tidak cukup hanya menjadi negara yang semakin digital. Indonesia harus menjadi negara digital yang aman, tangguh, dapat dipercaya, dan mampu pulih ketika diserang.

Keamanan siber memang tidak selalu terlihat ketika bekerja dengan baik. Namun, tanpa keamanan siber, seluruh hasil pembangunan digital dapat berhenti dalam sekejap.

Karena itu, keamanan siber bukan biaya tambahan. Ia adalah investasi untuk menjaga agar pembangunan tetap berjalan, pelayanan tetap tersedia, ekonomi tetap bergerak, data rakyat tetap terlindungi, dan negara tetap berdaulat.

Jakarta, 18 Juli 2026

Dr. Ir. Hendri, ST., MT
Wartawan Utama
Ketua Umum Jurnalis Nasional Indonesia (JNI)