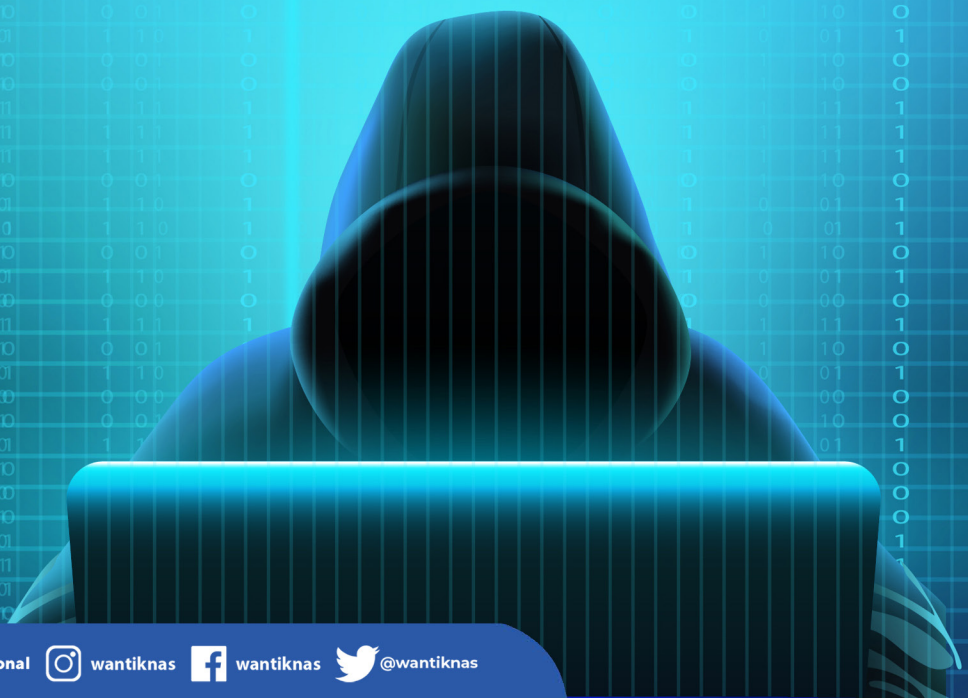
WANTIKNAS

Dewan Teknologi Informasi dan Komunikasi Nasional

MENJAWAB TANTANGAN KEAMANAN SIBER



Assalamualaikum Warrahmatullahi Wabarakatuh

Pembaca yang budiman, berdasarkan data National *Cybersecurity* Index (NCSI) 2023, Indonesia berada di peringkat ke-48 dengan indeks 63,64. Terpaut 31,17 poin dari Belgia sebagai negara dengan keamanan siber terbaik. Padahal, menurut laporan We Are Social, jumlah pengguna internet di Indonesia telah mencapai 213 juta orang per Januari 2023. Jumlah ini setara 77% dari total populasi Indonesia sebanyak 276,4 juta orang pada awal tahun ini. Dengan angka pengguna internet demikian tinggi dan indeks keamanan siber rendah, berarti negara kita masih belum mampu mengatasi serangan siber dengan baik dan ini bukanlah kondisi yang bagus.

Dengan rendahnya indeks keamanan siber Indonesia, maka kita berpotensi untuk mendapatkan kendala dalam dunia bisnis. Dalam pertemuan World Economic Forum 2023 di Davos, Swiss didapati fakta bahwa separuh dari para pemimpin bisnis berencana untuk mengevaluasi ulang negara-negara yang melakukan bisnis dengan mereka karena mereka percaya bahwa ketika berbisnis dengan organisasi atau pemerintah yang kebijakan dan keamanan sibernya kurang, maka akan mewarisi risiko dalam bisnis.

Bukan tanpa upaya, kita semua tahu pemerintah telah melakukan banyak hal untuk mengatasi berbagai ancaman serangan siber walau masih belum sempurna. Lewat e-Buletin edisi ini, Wantiknas mencoba ingin melihat bagaimana kondisi keamanan siber Indonesia sebenarnya dan apa yang harus dilakukan. Dengan semakin berkembangnya teknologi tentu saja upaya pencegahan dan penanganan serangan siber juga harus terus disempurnakan.

Tentu ini tidak hanya menjadi tanggung jawab satu lembaga saja, melainkan semua pihak yang berkepentingan. Kolaborasi dari *multistakeholder* akan menghasilkan formulasi pencegahan dan penanganan yang paripurna. Bukan untuk jangka pendek semata melainkan untuk masa yang akan datang termasuk mempersiapkan pakar-pakar keamanan siber masa depan. ●

Jabat Erat

Dr. Ing. Ilham Akbar Habibie, M.B.A.

Ketua Tim Pelaksana WANTIKNAS

Diterbitkan oleh
Dewan TIK Nasional

Redaksi:
Tim Humas WANTIKNAS

WANTIKNAS
Dewan Teknologi Informasi dan Komunikasi Nasional
Graha Jasindo Lt. 6
Jl. Menteng Raya No.21, Jakarta Pusat
Daerah Khusus Ibukota Jakarta 10340
Telp : 021-39831983

sekretariat@wantiknas.go.id

Daftar isi

Dewan TIK Nasional dideklarasikan pada 13 November 2006 oleh Presiden Republik Indonesia saat itu, Susilo Bambang Yudhyono. Dewan yang disebut oleh presiden sebagai kelompok kerja yang dibentuk untuk mendorong pembangunan teknologi informasi dan komunikasi Indonesia ini sesungguhnya bukanlah lembaga yang benar-benar baru.

Jauh sebelumnya, pada 31 Juli 1997, Pemerintah Indonesia yang saat itu dipimpin oleh Presiden Soeharto membentuk apa yang disebut Tim Koordinasi Telematika Indonesia (TKTI) melalui Keputusan Presiden No. 30 Tahun 1997 TKTI. Selanjutnya penyempurnaan demi penyempurnaan TKTI dilakukan oleh pemerintahan-pemerintahan setelahnya. Namun dengan pertimbangan bahwa Tim Koordinasi Telematika Indonesia yang telah dibentuk, dipandang sudah tidak sesuai lagi dengan perkembangan keadaan maka pada masa Presiden Susilo Bambang Yudhoyono dibentuklah Wantiknas.

Jika sebelumnya TKTI diketuai oleh Wakil Presiden, Menteri Kordinator, bahkan Menteri Negara, namun pada Keppres No. 20 Tahun 2006 disebutkan Wantiknas langsung diketuai oleh Presiden RI dengan Ketua Pelaksana Harian, Menteri Negara Komunikasi dan Informatika.

Mengacu Keppres No. 20 Tahun 2006 yang dikeluarkan pada tanggal 11 November 2006, tugas utama Wantiknas adalah merumuskan kebijakan umum dan arahan strategis pembangunan nasional melalui pendayagunaan TIK. Wantiknas mengemban tugas menyiapkan cetak biru dan *roadmap* TIK Indonesia guna menentukan arah perkembangan langkah-langkah yang harus ditempuh guna mewujudkan masyarakat Indonesia berbasis pengetahuan pada 2025. Target tersebut menuntut pembangunan jaringan komunikasi bagi 43 ribu desa di tanah air yang hingga kini belum memiliki jaringan telekomunikasi tetap. Jaringan telekomunikasi juga dibutuhkan bagi 31.173 SMP dan SMA, serta 2.428 perguruan tinggi, serta 28.504 pusat kesehatan masyarakat.

Kemudian lembaga Wantiknas kembali mengalami penyempurnaan lewat Keppres No. 1 Tahun 2014 yang menyempurnakan tugas dan susunan keanggotaan Wantiknas. Dengan Ketua Tim Pengarah yang dijabat oleh Presiden RI dan Ketua Tim Pelaksana yang dijabat oleh Dr. Ing. Ilham Akbar Habibie, M.B.A.

Tugas WANTIKNAS Menurut Keppres No.1 Tahun 2014

- Merumuskan kebijakan umum dan arahan strategis pembangunan nasional, melalui pengembangan teknologi informasi dan komunikasi termasuk infrastruktur, aplikasi dan konten.
- Melakukan pengkajian dalam menetapkan langkah-langkah penyelesaian permasalahan strategis yang timbul dalam rangka pengembangan teknologi informasi dan komunikasi.
- Melakukan koordinasi nasional dengan instansi Pemerintah Pusat / Daerah, Badan Usaha Milik Negara / Badan Usaha Milik Daerah, Dunia Usaha, Lembaga Profesional, dan komunitas teknologi informasi dan komunikasi, serta masyarakat pada umumnya dalam rangka pengembangan teknologi informasi dan komunikasi.
- Memberikan persetujuan atas pelaksanaan program pengembangan teknologi informasi dan komunikasi yang bersifat lintas kementerian agar efektif dan efisien.

Tugas Tambahan WANTIKNAS Menurut Keputusan Menteri PPN/Kepala Bappenas Nomor Kep.86/M.PPN/HK/07/2021"

- Pengembangan Transformasi Digital

MENJAWAB TANTANGAN KEAMANAN SIBER

Seiring dengan instabilitas ekonomi dan geopolitik yang meluas dalam beberapa tahun terakhir, para ahli memprediksi bahwa tahun 2023 akan menjadi tahun yang penting dalam bidang keamanan siber. Perkembangan yang mereka sebutkan akan mencakup lanskap ancaman yang semakin luas dan serangan siber yang semakin canggih. Untuk itu, pemerintah memerlukan sebuah langkah serius untuk mengantisipasi ini. Selain langkah yang tepat, program edukasi juga perlu bagi masyarakat.

Dalam pertemuan World Economic Forum 2023, di Davos, Swiss yang fokus membahas persoalan keamanan siber disebutkan bahwa 93% pakar keamanan siber dan 86% pemimpin bisnis percaya bahwa dalam dua tahun yang akan datang serangan siber menjadi sangat marak dan berdampak parah.

Pertemuan ini juga mencatat bahwa adopsi perangkat yang terhubung selama masa pandemi beberapa tahun lalu telah menyebabkan peningkatan serangan siber yang dramatis dan jika dibiarkan tanpa pengendalian maka akan mengakibatkan biaya serangan siber terus meningkat, serta mengancam ekonomi global yang rapuh.

Indonesia sendiri telah merasakan apa yang telah diprediksikan oleh para pakar di pertemuan Davos. Menurut Gubernur Lembaga Ketahanan Nasional (Lemhannas) Andi Widjajanto dalam Seminar Ketahanan Nasional Transformasi Digital Indonesia 2045 pada awal Agustus 2023 lalu, Indonesia mengalami 2.200 serangan siber anomali tiap satu menit pada tahun 2023. Sementara pada tahun 2022, serangan siber anomali yang terdeteksi mencapai 1,2 miliar. Jumlahnya kian meningkat dibandingkan sebelum pandemi Covid-19 yaitu 400 juta per tahun.

"Indonesia mengalami 2.200 serangan siber. Anomali-anomali seperti itu, 2.200 per menit di Indonesia," kata Andi sebagaimana dikutip dari Kompas.

com. Andi mengungkapkan, serangan siber anomali ini beragam. Biasanya, serangan menyasar data-data pribadi, data-data korporasi, data-data niaga hingga data lainnya.

Sementara berdasarkan laporan AwanPintar, ada 347,17 juta serangan digital terjadi di Indonesia sejak Januari hingga Juni 2023. Jumlah itu didapat dari rata-rata serangan terhadap sebuah sensor yang telah dipasang di sejumlah jaringan internet. Melihat trennya sepanjang tahun ini, serangan digital sempat mengalami penurunan hingga April 2023. Namun, jumlahnya kembali melonjak menjadi 112,66 juta kasus pada Mei 2023. Lonjakan tersebut seiring terjadinya kasus *ransomware LockBit* di dalam negeri, salah satunya menimpa Bank Syariah Indonesia (BSI) pada awal Mei 2023.

Masalah ancaman siber ini juga diakui oleh Ketua Indonesia *Cyber Security* Forum (ICSF), Ardi Sutedja, sayangnya menurut Ardi kasus-kasus serangan siber ini seringkali tidak mendapatkan perhatian yang serius.

"Kita memang punya masalah ancaman siber, dan masalah tersebut tidak pernah dikupas dan tidak dituntaskan. Sementara banyak pakar-pakar tanpa jam terbang yang ngomong kiri kanan dan yang *expert* memiliki pengalaman di lapangan di Indonesia bisa dihitung dengan jari," ujar Ardi saat diwawancarai oleh Tim Humas Wantiknas.

Potensi Ancaman Siber Indonesia

Menurut jenisnya, aktivitas internet yang anomali atau mencurigakan menjadi jenis serangan paling banyak ditemui di Indonesia. Kasus dengan istilah *misc activity* itu ditemukan sebanyak 119,94 juta serangan sejak Januari-Juni 2023.

Ada pula aktivitas ilegal dengan melibatkan pendeteksian semua *host* aktif di jaringan dan memetakannya ke alamat IP sebanyak 92,79 juta serangan. Kemudian, sebanyak 55,47 juta serangan berupa anomali di paket data protokol jaringan yang tidak diharapkan atau tidak sah.

Lebih lanjut, Brasil menjadi negara yang paling sering melakukan serangan siber ke Indonesia. Selain itu, serangan siber ke Indonesia juga banyak bersumber dari Amerika Serikat dan China.

Sementara Badan Siber dan Sandi Negara (BSSN) pernah memprediksikan bentuk ancaman siber di Indonesia pada 2023. Diprediksi ancaman siber yang akan terjadi pada 2023, mulai dari *ransomware*, kebocoran data, *phising*, sampai *social engineering.* Dalam seminar bertajuk "Cyber Challenges and Threats in Indonesia" yang diadakan The Iconomics pada 27 Juni 2023, Direktur Keamanan Siber dan Sandi Keuangan Perdagangan dan Pariwisata BSSN, Edit Prima mengatakan bahwa di tahun 2023 sampai dengan bulan Mei ini tercatat ancaman *malware* yang mendominasi.

"Nah ini data tahun 2023 sampai dengan bulan Mei memang tercatat *malware, malware* secara umum ya ini mendominasi hampir 60%, *ransomware* juga bagian dari kategori *malware* jadi bisa dibayangkan inilah katakanlah prediksi yang relatif akurat dari (yang) teman-teman buat di awal tahun," ucap Edit

Adapun persebaran berdasarkan pemantauan *anomaly traffic* hingga Mei 2023 ini yaitu *malware* sebesar 57,5%, *Trojan Activity* 26,83%, *Information Leak* 6,34%, lain-lain 6,25%, Exploit 1,68%, APT 0,50%, *Denial of Service* 0,33%, *Web Application Attack* 0,27%, dan *Information Gathering* 0,55%.

Perlu Perhatian Serius dan Kolaborasi

Maraknya serangan siber ke Indonesia ini, memunculkan pertanyaan, sebarapa siap kita menghadapi serangan-serangan siber di masa yang akan datang. Karena angka 347,17 juta serangan digital terjadi di Indonesia sejak Januari hingga Juni 2023 tidak bisa dianggap remeh, terlebih juga menyasar ke lembaga-lembaga pemerintah yang di dalamnya terdapat rahasia negara berarti juga mengancam kedaulatan negara.

Sebagaimana data dari BSSN, pada tahun 2022 lalu, mayoritas target serangan siber ke Indonesia menyasar sektor administrasi pemerintahan pada tahun lalu. Jumlahnya tercatat sebanyak 284,09 juta serangan dan 1,7 juta serangan siber yang menyasar ke sektor pertahanan pada 2022. Jika tidak segera melakukan langkah antisipasi, maka dalam waktu singkat kedaulatan dan keamanan digital akan tumbang dan pada akhirnya hanya menjadi "bancakan" baik oleh negara besar maupun pelaku kejahatan digital.

Menurut Ardi Sutedja, persoalan keamanan siber ini memang tidak bisa hanya dilakukan secara parsial karena sudah menjadi masalah program nasional. Sayangnya menurut Ardi hingga saat ini belum ada yang berbicara bahwa keamanan siber ini masuk ke ranah pertahanan nasional yang sangat strategis. Hal ini disebabkan oleh cara melihatnya yang masih parsial dan tidak menyeluruh. Butuh kolaborasi *multistakeholder* dan harus dilakukan secara transparan berdasarkan sebuah strategi jangka panjang. Karena tantangan ke depannya akan menjadi semakin berat.

Ardi Sutedja
Ketua Indonesia *Cyber Security* Forum (ICSF)

"Apa yang terjadi pada BSI merupakan insiden siber nasional dan menjadi sebuah *game changer.* Kita sudah berhadapan dengan peretas lintas batas, kelas dunia, terorganisir dan sudah masuk ke masa politik dan mengancam keamanan. Ini harus ditanggapi secara serius bukan hanya oleh satu lembaga, tapi seluruh *stakeholder* yang berkepentingan. Kita memang memiliki BSSN, tapi BSSN ini lembaga baru dan kita masih belajar," tambah Ardi.

Selain itu, Ardi juga menilai pemerintah perlu lebih transparan kepada masyarakat dalam hal penanganan kebocoran data sehingga dapat menjaga integritas dan kepercayaan publik terhadap sistem keamanan siber di Indonesia.

"Kepercayaan publik terhadap sistem digital yang sedang berjalan itu perlu dijaga sehingga dalam penanganan kebocoran data perlu mengedapankan transparansi. Sehingga masyarakat melihat ada ketegasan dari regulator dan ini menunjukkan integritas (pemerintah) kepada publik," ujar Ardi lagi.

Selama ini dalam kasus-kasus dugaan kebocoran data yang terjadi beberapa tahun terakhir, pemerintah dinilai belum terbuka dalam hal penanganan kasus-kasus tersebut dan membuat masyarakat mulai kehilangan kepercayaan. Maka dari itu, dengan adanya Undang-Undang nomor 27 tahun 2022 tentang Pelindungan Data Pribadi (PDP) yang saat ini tengah disusun regulasi turunannya, Ia berharap transparansi dan publikasi penanganan kasus kebocoran data bisa diatur lewat regulasi tersebut.

Sementara Anggota Tim Pelaksana Wantiknas yang juga CEO Allo Bank, Indra Utoyo membagikan resep yang telah ia terapkan dalam menangani persoalan *cyber security.* Indra bercerita jika bank digital yang dipimpinnya menerapkan *framework* dari *the National Institute of Standards and Technology* (NIST). "Framework dari NIST ini membagi penanganan keamana siber menjadi dua hal. Pertama bagaimana men-*defence* sekuat-kuatnya, kemudian yang kedua me-*recovery* sekuat-kuatnya jika terjadi masalah," jelas Indra.

Indra menjelaskan ada lima pilar dalam *framework* NIST tersebut, yang pertama adalah identifikasi aset termasuk data apa yang harus diproteksi dengan sangat ketat. Kemudian yang kedua proteksi, bagaimana melakukan proteksi semaksimal mungkin sesuai standar teknologi, prosedur dan kompetensi orangnya harus awal memang itu dan harus selalu diperbaharui setiap data ada mekanisme proteksi data. Ketiga, deteksi, bagaimana kita bisa mendeteksi secara dini, melakukan *action* atau penutupan atau *blocking.* Keempat, respon yang cepat, actionnya juga harus sangat *actionable* sampai ke bawah tidak boleh gagap. Terakhir, *recovery*.

"Dengan *framework* yang jelas, maka setiap persoalan dalam keamanan siber baik di level antisipasi sampai penanganan serangan akan menjadi lebih efektif. Mungkin *framework* seperti ini yang harus kita pikirkan atau kita buat bersama" tambah Indra.

Baik Indra maupun Ardi tampak sejalan jika persoalan keamanan siber itu tidak bisa hanya diserahkan pada satu lembaga saja, melainkan harus ada kolaborasi dan koordinasi antar lembaga yang berkepentingan mulai dari Kepolisian RI, OJK, Kementerian Pertahanan, Kemenkominfo, Kementerian Keuangan, BSSN, dan lembaga lainnya.

Peningkatan Sumber Daya Mansusia dan Penelitian

Selain persoalan kordinasi, transparansi dan *framework*, ketersediaan SDM yang mumpuni juga menjadi kunci dari upaya mencegah serangan siber. Kebutuhan SDM ini ditegaskan oleh Ardi Sutedja karena menurutnya, kendati kita memiliki banyak SDM siber, namun rata-rata masih belum berpengalaman. "Selain itu, walaupun SDM siber kita banyak, tapi mereka masih minim jam terbang," ujarnya.

Ardi menegaskan dalam manajemen keamanan siber ada tiga hal yang harus dibangun dan perhatikan yaitu *people, process,* dan *technology.* Dengan demikian percepatan perkembangan digital saat ini juga perlu diimbangi dengan kemampuan dan kualitas SDM. Mengikuti perkembangan teknologi adalah sebuah kesemestian, namun jangan juga meninggalkan faktor SDM.

"Masalah peningkatan keamanan siber perlu memperhatikan pembangunan SDM, kultur, disiplin, pemahaman tata kelola, dan kepatuhan yang mengacu

kepada praktik-praktik keamanan siber secara global. Tidak kalah penting juga harus ada ketersediaan anggaran untuk membangun semua hal tersebut," paparnya.

Pentingnya SDM berkualitas juga diungkapkan oleh Indra Utoyo. Menurutnya keamanan siber itu bukan semata soal teknologi tapi juga termasuk *people* atau SDM. Teknologi itu hanya sebatas *tools* yang akan menjadi sia-sia jika SDM yang mengelola tidak sesuai prosedur dan kurang disiplin.

"SDM adalah faktor yang paling penting. Dalam persoalan *cyber security* bukan hanya tentang teknologi tapi juga *people*. Kita sering terjebak hanya pada persoalan teknologinya saja, seperti isu bahwa *cloud* itu tidak *secure* sementara data center lebih *secure*. Sebenarnya tidak begitu, padahal itu hanya *tools* yang lebih penting adalah kedisiplinan dalam tata kelola sudah diterapkan. Serta memastikan bahwa semua proses *tools* dan polanya sudah menerapkan semua prosedur " terang Indra.

Tidak jauh berbeda dengan Indra dan Ardi, Penasihat Senior Federasi Teknologi Informasi Indonesia yang juga anggota Tim Pelaksana Wantiknas Sylvia W. Sumarlin berpendapat, selain persoalan SDM yang harus mendapatkan perhatian adalah penelitian terkait isu keamanan siber.

"Isu seputar *cyber security* ada beberapa hal, tetapi masyarakat di Indonesia rata-rata hanya berbicara jaringan dan aplikasi. Padahal ada komponen penting yang hilang dan jarang menjadi bahan pembicaraan yakni penelitian. Di Indonesia belum ada penelitian terkait *cyber security* untuk kepentingan kita. Padahal hal tersebut saling terkait," terangnya.

Hilangnya kegiatan riset dari agenda terkait keamanan siber ini membuat Indonesia menjadi tidak siap dengan perkembangan seputar isu tersebut dan SDM yang ada tidak memiliki kemampuan memprediksi tren beberapa tahun ke depan.

"Padahal jika kegiatan riset mendapatkan perhatian maka pemangku kebijakan akan mengetahui arah teknologi 5-10 tahun kedepan seperti apa atau sudah ada gambaran beberapa tahun lagi akan kearah mana," lanjut Sylvia.

Dirinya juga berharap dengan meningkatnya *awareness* para pemangku kebijakan dan kepentingan dapat mendorong diadakan penelitian bersama tentang digital.

Baik Ardi, Indra maupun Sylvia sama-sama sepakat jika persoalan keamanan siber ini sudah seharusnya masuk ke dalam dunia pendidikan. Hal ini

Sylvia W. Sumarlin
Anggota Tim Pelaksana WANTIKNAS

untuk meningkatkan literasi di masyarakat dan untuk memenuhi kebutuhan SDM yang berkualitas.

Anak-anak perlu diingatkan tentang risiko yang menyertai semua aplikasi ponsel pintar dan komputer yang dipakai mereka. Minimal, setiap anak mengetahui bagaimana menjaga kerahasiaan informasi mereka, menahan diri tidak menanggapi orang tak dikenal, dan melaporkan sesuatu yang tak biasa kepada orang dewasa. Kurikulum tentang keamanan siber juga menjadi upaya pemenuhan kebutuhan SDM keamanan siber yang mumpuni. Kurikulum ini harus terus berkembang seiring dengan perkembangan teknologi dan kebutuhan dari dunia usaha dan pemerintahan.

Mungkin kita agak tertinggal soal keamanan siber, tapi bukan berarti kita tak mampu mengejar. Tak pelak, untuk mengharmonisasi atau mengorkestrasi langkah pengamanan siber dibutuhkan satu strategi siber nasional yang menjadi panduan bagi seluruh stakeholder baik pemerintahan, industri, maupun dunia pendidikan. Dengan strategi siber nasional, kita akan memiliki formula dan *framework* yang paling tepat untuk Indonesia baik jangka pendek maupun jangka panjang. Tinggal kita sepakati bersama, kapan kita akan memulai.●

Regulasi dan Sumber Daya Manusia Perkuat Keamanan Siber Nasional

Sepanjang tahun 2023, setidaknya terjadi 2.200 serangan siber. Hal tersebut disampaikan langsung oleh Gubernur Lembaga Ketahanan Nasional. Bahkan, baru-baru ini kasus yang cukup menjadi sorotan adalah sektor bank, yakni Bank Syariah Indonesia (BSI) yang terkena hack. Sehingga merugikan berbagai pihak. Bagaimana seharusnya dalam menjaga keamanan siber? Simak wawancara Tim Humas Wantiknas dengan Anggota Tim Pelaksana Wantiknas, Indra Utoyo, berikut ini.

Berdasarkan laporan National *Cyber Security* Indeks, skor keamanan siber di Indonesia 38,96 dari 100 atau peringkat 83 dari 160 negara atau ke 6 di Asia Tenggara, sebenarnya seperti apa kondisi keamanan siber di Indonesia saat ini?

Banyaknya serangan siber di dunia, termasuk negara kita Indonesia sudah banyak kasusnya, contohnya seperti yang terjadi pada Bank Syariah Indonesia (BSI) kemarin. Kita juga merasakan ancaman di sini, terlebih pertukaran data rentan terjadi. Menariknya, *social engineering* yang terjadi di masyarakat sangat luar biasa. Sayangnya, masyarakat kita juga memang mudah percaya orang. Hal ini membuat *social engineering* menjadi salah satu yang berkembang.

Terkait BSI yang terkena *hack*, apa faktor yang menyebabkan ini terjadi? Lalu apa yang menjadi kelemahannya?

Pada kasus ini, BSI lemah pada dua sisi, yakni *defence* yang lemah dan *recovery* yang lambat. Di era digital ini perlu cepat dan *recovery*, kalau hal tersebut tidak segera diatasi akan terjadi *framing* yang liar dan tidak dapat ditutupi lagi. Maka yang perlu dilakukan adalah dengan memperbarui regulasi lebih cepat karena hal tersebut penting. Apabila tidak segera dilakukan, media saat ini sangat cepat dan berdampak pada liarnya pemberitaan.

Kelemahan terbesar dari sisi keamanannya adalah tetap pada faktor *human* bukan dari teknologi. Terkadang dari nasabah yang kurang kesadaran untuk melindungi data pribadinya. Bahkan, bisa juga penjahatnya menggunakan kecerdasan buatan dan hal tersebut yang terjadi di perbankan. Jika kesalahannya pada *customer*, maka perlu diberikan edukasi dan bisa secara industri karena tidak bisa

sendirian. Kemudian kelemahan terbesar pada manusia yakni seberapa aman dan baik pun sistem yang dibangun, tetapi jika orangnya tidak *aware* terhadap keamanan dan *password*-nya, maka akan sama saja.

Bagaimana standar keamanan siber yang perlu diimplementasikan untuk mengatasi hal tersebut?

Terkait dengan *cyber security*, *framework*-nya yang lazim dipakai yaitu dari *National Institute of Standards and Technology* (NIST) yang terdiri dari lima tahapan dengan tujuan men-*defence* sekuat-kuatnya kalau terjadi masalah dan me-*recovery* secepatnya. **Pertama**, identifikasi aset apa yang paling berisiko untuk diproteksi, pasti pada akhirnya yang diserang data, intinya dari *cyber security*, terkait data apa saja yang harus diproteksi sangat ketat harus ditetapkan selanjutnya. **Kedua**, proteksi, bagaimana melakukan proteksi semaksimal mungkin ada standar teknologi, prosedur dan kompetensi orangnya dan harus selalu diperbaharui setiap data ada mekanisme proteksi data. **Ketiga**, deteksi bagaimana kita bisa mendeteksi secara dini, melakukan *action* atau penutupan atau *blocking*. **Keempat**, respon yang cepat, tindak lanjutnya juga harus sangat *actionable* sampai ke bawah tidak boleh gagap. **Kelima**, *recovery*.

Bagaimana dengan pemerintah, apa yang harus dilakukan? Apakah selama ini berjalan baik peraturan maupun kelembagaannya?

Berbagai macam upaya telah dilakukan. Otoritas Jasa Keuangan (OJK) khususnya Bank Indonesia (BI) sudah mengatur supaya tata kelola kita terkait proteksi data, *cyber security* itu semakin meningkat kepatuhannya. Selain itu, juga terkait digital yang didorong adanya digital *maturity*.

Apakah sistem keamanannya atau Sumber Daya Manusia (SDM) yang kurang berkualitas?

Faktor SDM paling penting, dan keamanan bukan hanya teknologi, tetapi sumber daya manusia. Misalnya, kita sering terjebak pada *cloud* yang tidak aman, tetapi data center lebih aman. Padahal, sebenarnya tidak begitu, tetapi lebih kedisiplinan dalam tata kelola yang diterapkan. Selain itu, perlu memastikan bahwa proses dan polanya sudah menerapkan semua prosedur dan ada hal yang harus dilakukan.

Lebih dari itu, ada kemampuan dan hal penting yang perlu dibangun dari sebuah organisasi. Tidak hanya sekedar teknologi yang bagus, tetapi SDM yang kemudian menjadi sebuah sistem untuk diterapkan dengan disiplin ISO 2013 dan ditambah 2022. Saya rasa itu menjadi kalibrasi yang sudah memenuhi kaidah-kaidah sistem keamanan dengan baik. Membangun kedisiplinan pada tata kelola yang baik menjadi investasi yang perlu dilakukan.

Menurut Anda, kita bicara kurikulum seperti apa yang seharusnya diadakan atau dipersiapkan dalam Kemdikbud?

Era digital mendorong kurikulum terus berkembang, tidak hanya pada teknologi, namun tata kelola, wawasan, tindakan, dan strategi pemenuhannya harus dikembangkan. Terkait SDM, sudah pasti ada yang organisir, perlu diperkuat dengan desainer arsitektur, *testing quality, identity,* dan vendor yang memang harus memiliki spesialisasi di bidang tersebut. Sehingga ketika ada serangan, bisa langsung dilakukan audit forensik dengan memakai pihak ketiga. Pada intinya yang dibutuhkan saat ini, perlu ada kurikulum terbaru tentang *cyber security.*

Kolaborasi Pentahelix Ciptakan Strategi Keamanan Siber untuk Kedaulatan

Internet telah merubah dunia. Dimulai dari pemakaiannya terbatas di dunia militer, lalu berkembang ke bisnis, pemerintahan dan berevolusi sangat cepat di kehidupan sehari-hari masyarakat.

Cybersecurity threat atau ancaman keamanan siber adalah ancaman serangan jahat yang dilakukan oleh individu atau organisasi yang mencoba mendapatkan akses ke jaringan komputer, merusak data, atau mencuri informasi rahasia. Ancaman keamanan informasi adalah serangan yang berkaitan langsung dengan pemangku kepentingan TI dan jaringan komputer organisasi Anda.

Pelaku itu disebut sebagai *Malicious actors.* Aktifitas *malicious actors* mulai dari melakukan gangguan diikuti dengan ancaman dan perusakan. Sudah banyak yang menjadi korban, termasuk di negara kita. Korbannya adalah perorangan dan institusi baik itu lembaga pemerintahan, sosial maupun bisnis.

Malware masuk ke perangkat komputer maupun gadget, ada yang melakukan aksinya saat itu juga dan yang menetap berhari-hari baru melakukan aksi perusakannya sampai ke spionase dan pencurian kekayaan intelektual. Perusakan kepada infrastruktur kritis (seperti perbankan, rumah sakit, pemerintahan) dan sampai melakukan pemerasan dengan meminta tebusan. Belakangan ini, ramai terjadinya pencurian data pribadi dan pembobol mengancam atau meminta tebusan agar data tidak dibocorkan. Modus lain pembobol tidak meminta tebusan, tapi langsung menjual data pribadi ke pihak-pihak yang ingin mendapatkannya.

Dengan situasi yang demikian bahaya, menurut saya sudah saatnya pemerintah mempunyai suatu strategi, peta jalan dan rencana aksi. Serangan-serangan *malware* yang sudah terjadi belakangan ini saya duga juga tumbuh secara eksponensial.

Salah satu konten dari peta jalan itu selayaknya berisi konsep reaktif dan antisipatif. Reaktif seperti penanganan (pemadaman) "fraud", dimulai dari proses pelaporan dari “fraud” yang datang dari masyarakat dan institusi yang ditujukan ke suatu *response center* terpadu. Kemudian laporan yang diterima di *response center* ini secara otomatis dan cepat langsung ditangani oleh badan/lembaga/organisasi yang bertanggung jawab untuk menanganinya. Untuk penanganan antisipatif diperlukan *think-thank* dan riset dari para ahli untuk melihat ancaman masa depan dan konsep untuk menghindarinya (*preventive*).

Hari Sungkari
Anggota Tim Pelaksana Wantiknas

Jangka waktu pembuatan peta jalan ini menurut saya adalah “*urgent*”, setidaknya dalam waktu kurang dari satu tahun Indonesia sudah memilikinya. Pembuatan peta jalan ini harus melibatkan *multi-stakeholder*, yakni pemerintah, bisnis, akademisi, komunitas dan *lead*-nya ada di pemerintah. Mari kita bersama-sama memberikan masukan agar peta jalan ini segera selesai sehingga negara kita tetap mandiri dan terjaga kedaulatannya. ●

WANTIKNAS
Dewan Teknologi Informasi & Komunikasi Nasional

KONDISI KEAMANAN SIBER DI INDONESIA SAAT INI DAN REKOMENDASI STRATEGI KEAMANAN SIBER NASIONAL

Keamanan siber merupakan tantangan terbesar di Indonesia. Beberapa waktu lalu, berita terkait kasus pembobolan data marak dilakukan. Tentunya, tidak asing dengan nama Bjorka, dan terakhir adalah kasus yang terjadi pada sektor perbankan yang di-*hack* atau kasus pencurian data Bank Syariah Indonesia (BSI) pada Mei 2023. Selain peningkatan kesadaran terhadap penggunanya, perlu juga regulasi yang mendorong tata kelola keamanan data.

PREDIKSI ANCAMAN SIBER DI INDONESIA TAHUN 2023

DATA BREACH

SERANGAN RDP

WEB DEFACEMENT

RANSOMWARE

PHISHING

CRYPTOJACKING

DDOS

JUMLAH SERANGAN SIBER DI INDONESIA (JANUARI JUNI 2023)

Januari	Februari	Maret	April	Mei	Juni
62,09%	53,82%	44,64%	36,79%	112,66%	37,18%

Berdasarkan rata-rata serangan terhadap sebuah sensor yang dipasang di sejumlah jaringan internet. Sejak Januari hingga Juni 2023 ada 347,17 juta serangan digital terjadi di Indonesia.

KEBIJAKAN DAN REGULASI KEAMANAN SIBER DI INDONESIA

- **Perpres Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital**
- **Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber**

NIST FRAMEWORK

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Sumber: BSSN, Dataindonesia & Awan Pintar, NIST

WANTIKNAS
Dewan Teknologi Informasi dan Komunikasi Nasional

Dewan Teknologi Informasi dan Komunikasi Nasional
Graha Jasindo Lt.6, Jl. Menteng Raya No.21, Jakarta Pusat
Daerah Khusus Ibukota Jakarta 10340
Telp : 021-39831983

sekretariat@wantiknas.go.id