White Paper

PENTINGNYA KEMITRAAN UNTUK MEMPERKUAT KEAMANAN SIBER INDONESIA

CfDS
CENTER FOR DIGITAL SOCIETY

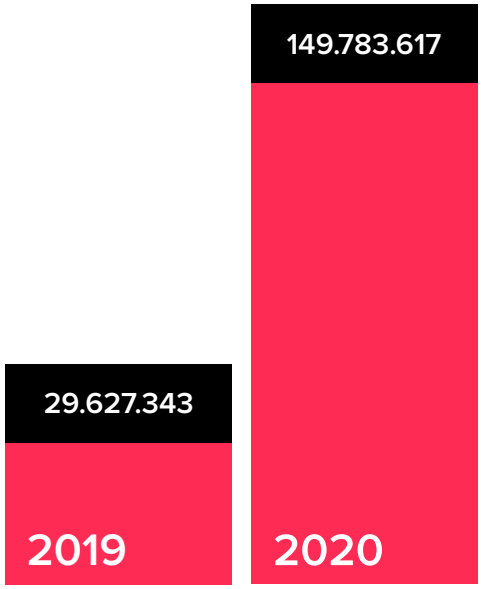
Kajian ini dipersembahkan oleh

RINGKASAN EKSEKUTIF

Permasalahan keamanan siber selalu ada dan berkembang.

Selama masa pandemi, dicatat adanya peningkatan akses yang menghasilkan gaya hidup digital baru. Berdasarkan survei Jakpat[1], 7 dari 10 orang mengklaim COVID-19 sebagai *game changer* dimana perpindahan aktivitas luring ke daring menjadi salah satu perubahan besar yang dialami.

Dengan meningkatnya aktivitas di internet ini, risiko terjadinya serangan siber semakin perlu diwaspadai. Menurut data dari Badan Siber dan Sandi Negara (BSSN), selama periode semester pertama tahun 2020, telah terdeteksi 149.783.617 serangan siber ke Indonesia. Jumlah ini lebih banyak bahkan hampir mencapai lima kali lipat dibanding periode semester satu tahun 2019 lalu yang berjumlah 29.627.343.[2]



(Sumber : Badan Siber dan Sandi Negara)

Gambar 1. Serangan Siber ke Indonesia periode semester satu 2019 -2010

Upaya serangan siber masih banyak dilakukan melalui platform media sosial dan komunikasi. Hal ini utamanya didukung oleh tingginya tingkat penggunaan media sosial melalui ponsel pintar.[3] Untuk menjamin kemajuan teknologi yang ada dapat bermanfaat bagi kemajuan dan kesejahteraan masyarakat Indonesia, keamanan ekosistem digital menjadi penting untuk dipertahankan. Kajian ini menekankan pentingnya kerjasama antar pemangku kepentingan untuk dapat mencapai hal tersebut.

Transparansi terhadap praktik dan kebijakan keamanan siber di tingkat perusahaan diperlukan.

Transparansi menjadi penting karena serangan siber tidak hanya berdampak pada kerugian materi dan hukum, tapi juga berpengaruh pada kepercayaan pemegang saham dan konsumen terhadap aset yang mereka miliki di perusahaan tersebut.

Hal seperti ini dilakukan oleh TikTok dengan didirikannya Pusat Transparasi dan Akuntabilitas[4] di Amerika Serikat dimana para ahli teknologi dan pemangku kepentingan termasuk pemegang kebijakan dapat melihat bagaimana Panduan Komunitas TikTok diterapkan dalam memoderasi konten, meninjau kode sumber TikTok serta praktik keamanan data dalam melindungi privasi dan informasi pengguna TikTok.

[1] Jakpat Survey Report (2020). New Normal : Life After COVID-19 - JAKPAT Survey Report 2020

[2] "Hadiri Rapat Kerja Teknis Kejaksaan Agung RI Bidang Intelijen, Kepala BSSN Ingatkan Budaya Keamanan Siber dan Pancasila Merupakan Kunci Kekuatan Bangsa Indonesia Hadapi Ancaman Serangan Siber" (Sept 2020) Badan Siber dan SandiNegara, [daring]. Tersedia di: https://bssn.go.id/hadiri-rapat-kerja-teknis-kejaksaan-agung-ri-bidang-intelijen-kepala-bssn-ingatkanbudaya-keamanan-siber-dan-pancasila-merupakan-kunci-kekuatan-bangsa-indonesia-hadapi-ancaman-serangan-siber/ (diakses pada: Oktober 2020)

[3] We Are Social Hootsuite (2020). Digital 2020: Indonesia. Datareportal, [daring]. Tersedia di: https://datareportal.com/reports/digital2020-indonesia (diakses: Oktober 2020).

[4] TikTok (2020). Transparansi di TikTok, [daring]. Tersedia di: https://www.tiktok.com/transparency?lang=id. (diakses pada: Oktober 2020)

Perilaku pengguna dalam berinteraksi di dunia digital menjadi salah satu faktor pendukung terbesar dari ekosistem digital yang bebas ancaman.

Beberapa aspek tentu perlu diperhatikan oleh pengguna dalam memilih platform digital mana yang ingin mereka gunakan, antara lain bagaimana platform tersebut mengutamakan keamanan pengguna, data, dan informasi.

Platform digital perlu mendukung pemberdayaan pengguna untuk berperan menjaga keamanan aktivitasnya. Sebagai contoh TikTok menyediakan panduan dan juga kontrol bagi pengguna untuk mengatur akunnya agar tetap aman dan nyaman, baik untuk mereka sendiri maupun untuk pengguna lainnya.

Berbagai risiko ini perlu diatasi melalui kerjasama berbagai pemangku kepentingan demi keamanan seluruh ekosistem digital lintas sektor.

Kerjasama itu diantaranya melalui kemitraan bersama pemerintah dalam mendukung lingkungan regulasi yang mengakomodasi keadaan industri terkini, serta pengembangan sumber daya manusia terhadap kemampuan siber. Pemangku kepentingan lainnya seperti industri, akademisi, komunitas atau organisasi masyarakat, dan penggunanya itu sendiri juga memiliki peran masing-masing dan perlu bekerjasama. Seluruh pemangku kepentingan ini pun berperan untuk mewujudkan transparansi dalam strategi keamanan siber, dengan memperhatikan berbagai langkah, seperti kepemimpinan dan regulasi, analisa dan manajemen risiko, pembangunan kapasitas dan kesadaran, serta kerjasama internasional.

Kolaborasi antar pemangku kepentingan inilah yang menjadi salah satu tujuan dari disusunnya kajian ini, untuk mewujudkan transparansi dalam meningkatkan keamanan siber baik di tingkat nasional maupun internasional.

Seperti contoh, dalam membangun infrastruktur keamanan terbaik di kelasnya, TikTok bekerja sama dengan perusahaan keamanan siber terdepan di dunia untuk memvalidasi kepatuhan TikTok terhadap standar keamanan yang diakui secara global seperti NIST CSF, ISO 27001 dan SOC2.

Kajian ini dibuat berdasarkan kerjasama antara Onno Center dan Center for Digital Society (CfDS) untuk melihat dan merekomendasikan sejumlah praktik peningkatan keamanan siber di industri, sekaligus meninjau praktik peningkatan keamanan siber oleh TikTok sebagai salah satu platform digital yang paling banyak digunakan saat ini.

1 PENDAHULUAN

Di tahun 2019, muncul berbagai berita yang melibatkan kasus pencurian data pengguna internet.

Sementara itu, Badan Siber dan Sandi Nasional (BSSN) sendiri mencatat, ada 88,4 juta serangan siber yang terjadi di Indonesia, selama Januari- April 2020. Sedangkan konsultan hukum industri perangkat lunak, *Business Software Alliance* (BSA) menyebutkan, 83% perusahaan di tanah air rentan diretas[5].

Dengan adanya pandemi COVID-19 ini, dimana kegiatan sekolah dan perkantoran dianjurkan untuk dapat dilakukan secara jarak jauh, pengguna internet tidak mempunyai pilihan lain kecuali untuk lebih berhati-hati dalam menggunakan situs atau internet secara umum.

88,4 juta

Serangan Siber di Indonesia Periode Januari - April 2020

(Sumber : Badan Siber dan Sandi Negara)

83%

Jumlah Perusahaan di Tanah Air diretas

(Sumber : Business Software Alliance)

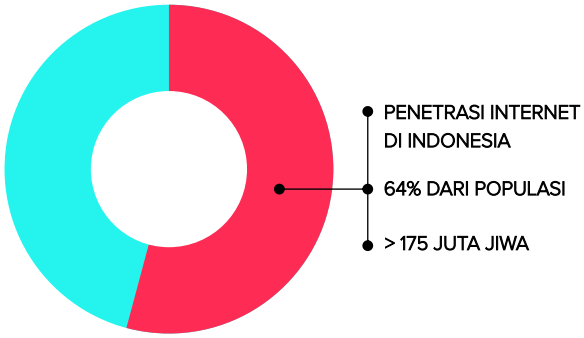
Serangan siber yang berpotensi semakin meningkat ini tidak hanya melibatkan pengguna individu, tetapi juga pemangku kepentingan yang lebih luas. Mulai dari perusahaan atau industri sebagai penyedia layanan jasa, sektor akademis yang mempersiapkan sumber daya manusia, dan juga pemerintah sebagai regulator, salah satunya dalam hal keamanan siber.

[5] Annur, Cindy Mutia (2020). "Ada 88,4 juta serangan siber, 83% perusahaan RI rentan diretas", Katadata, [daring]. Tersedia di : https://katadata.co.id/desysetyowati/digital/5f44d2505115c/ada-88-4-juta-serangan-siber-83-perusahaan-ri-rentan-diretas (Diakses pada : Oktober 2020)

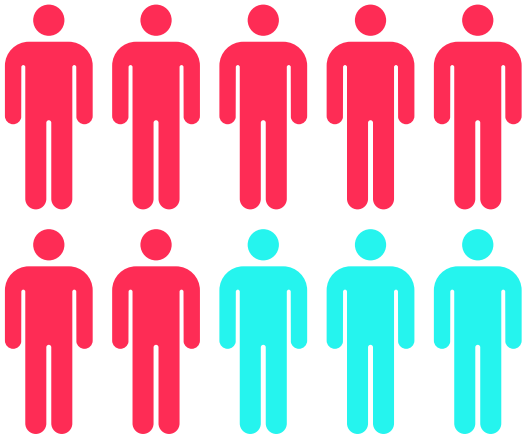
2 TREN DAN STATISTIK KEAMANAN

Indonesia mengalami peningkatan jumlah pengguna internet yang signifikan.

Menurut data dari We Are Social, Indonesia memiliki tingkat penetrasi internet sebesar 64% dari total populasi, dengan jumlah pengguna lebih dari 175 juta jiwa[6]. Sementara dari sisi penggunaan media sosial, Indonesia mengalami peningkatan yang tidak kalah signifikan di tahun 2020. Pengguna aktif media sosial meningkat sebesar 25 juta jiwa, dengan total 160 juta pengguna pada Januari 2020[7].



Gambar 2. Penetrasi Internet di Indonesia



Gambar 3. Survei Jakpat terhadap perubahan di masa pandemi

Selama masa pandemi, dicatat adanya peningkatan akses yang menghasilkan gaya hidup digital baru.

Berdasarkan survei Jakpat[8], 7 dari 10 orang di Indonesia mengklaim COVID-19 sebagai *game changer* dimana terdapat empat perubahan besar baru terkait dengan kebersihan pribadi, perpindahan aktivitas luring ke daring, kesadaran kesehatan dan menemukan hobi atau keterampilan baru.

[6] We Are Social Hootsuite (2020). Digital 2020: Indonesia. Datareportal, [daring]. Tersedia di: https://datareportal.com/reports/digital-2020-indonesia. (diakses pada: Oktober 2020)

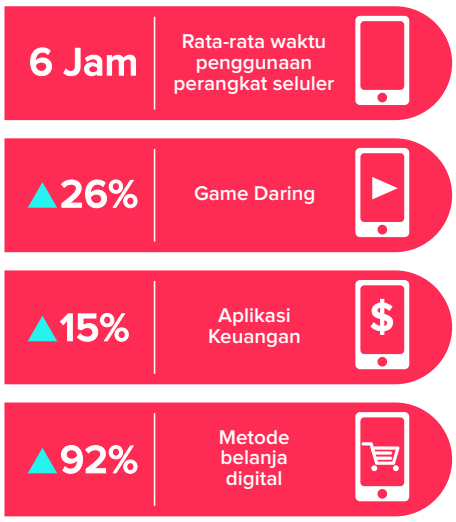
[7] ibid.

[8] Jakpat Survey Report (2020). New Normal : Life After COVID-19 - JAKPAT Survey Report 2020

Berdasarkan data Mckinsey[9] selama masa pandemi, Indonesia mengalami peningkatan penggunaan perangkat seluler dengan rata-rata waktu akses selama 6 jam sehari.

Selain itu, dicatat adanya: kenaikan 26% peningkatan waktu orang menghabiskan waktu untuk bermain game secara daring, serta peningkatan 15% rata-rata waktu dalam sebulan untuk mengakses aplikasi keuangan.

Peningkatan paling banyak terjadi pada perubahan metode belanja, yaitu 92% konsumen menyatakan telah mencoba metode belanja digital dan berencana akan terus menggunakan layanan walaupun masa pandemi telah usai.



Gambar 4. Data Mckinsey tentang perilaku digital masyarakat Indonesia selama pandemi.

Meskipun demikian, studi terkini dari Center for Digital Society (CfDS) bertajuk "*Higher Education 4.0 and the Readiness of Indonesia's Future Workforce*"[10] yang mengukur kesiapan mahasiswa Indonesia dalam memasuki dunia kerja 4.0 memperlihatkan hasil yang menarik.

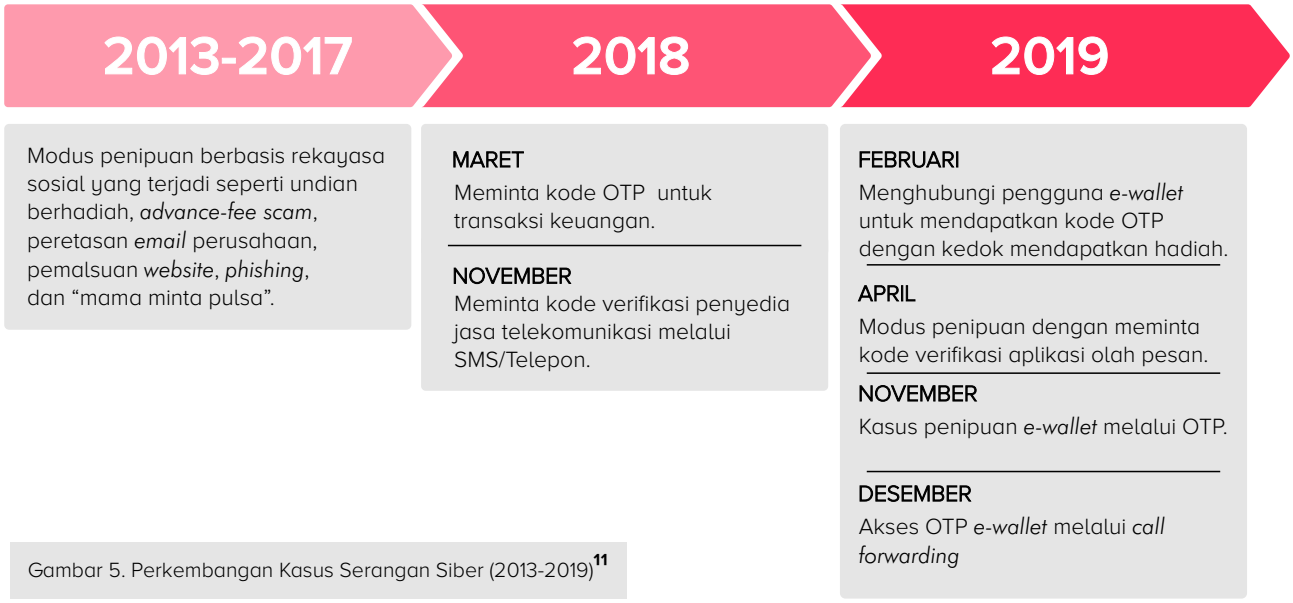
Hasil dari studi tersebut salah satunya adalah pengukuran terhadap kemampuan digital mahasiswa Indonesia, yang meliputi: pemrosesan informasi *(information processing)*, pembuatan konten *(content creation)*, keamanan *(safety)*, dan pemecahan masalah *(problem solving)*. Pemahaman dan kemampuan mahasiswa mengenai masing-masing dari kemampuan tersebut, selanjutnya diklasifikasikan ke dalam tiga level, yaitu dasar *(basic)*, menengah *(intermediate)*, dan lanjutan *(advance)*.

Hasilnya, dari survei 1.162 mahasiswa Indonesia, kemampuan dan pemahaman mengenai keamanan digital *(digital safety)* di Indonesia merupakan aspek dengan skor yang paling rendah apabila dibandingkan dengan kemampuan dan pemahaman digital lainnya. Kajian ini mencatat skor keterampilan terendah mahasiswa ada pada skill keamanan dengan skor 31,58 dari 100, untuk pemeriksaan fitur keamanan dan konfigurasi perangkat secara teratur.

[9] McKinsey. (2020). Survey: Indonesian consumer sentiment during the coronavirus crisis

[10] Mantovani, Anisa Pratita, Duanaiko, Anaq, Haryanto, Janitra, Putri, Treviliana Eka, Angendari, Dewa Ayu Diah. (2020). Higher Education 4.0 and the Readiness of Indonesia's Future Workforce. Center for Digital Society.

Selain itu, besarnya jumlah pengguna internet dan media sosial ini juga memunculkan perhatian khusus mengenai keamanan siber bagi pengguna dalam aktivitas digitalnya. Berdasarkan kajian CfDS dalam periode 2013-2019, di Indonesia, terdapat beberapa jenis kasus serangan siber yang paling sering terjadi, seperti terlihat dalam gambar berikut :



Gambar 5. Perkembangan Kasus Serangan Siber (2013-2019)[11]

Scam, Fraud, dan Hadiah Undian

Dalam melihat berbagai kasus tersebut, CfDS melakukan proses pencarian data dengan bersumber dari media press daring. Sedangkan untuk proses analisis, CfDS menggunakan teknologi *Big Data* dari Digital Intelligence Lab CfDS dengan menyasar pada kata kunci, diantaranya *scam, fraud*, bodong, penipuan, dan sebagainya. Dari data tersebut ditemukan bahwa kasus serangan siber paling banyak terjadi melalui modus pesan undian berhadiah dari aparat negara, perbankan, provider selular, hingga peretasan email.

Kemudian pada tahun 2014-2016, kasus *phishing* atau pemalsuan platform digital berbasis website atau aplikasi mulai marak terjadi. Sedangkan, kasus kejahatan siber yang memanfaatkan data pribadi mulai terjadi di tahun 2017 dengan pengambilan data melalui SMS, telepon, maupun media sosial.

Secara keseluruhan dalam periode 2013-2019, kasus penipuan dengan kedok hadiah undian masih terus berlangsung. Dengan tujuan untuk memperoleh data-data pribadi pengguna dengan mengirimkan *malware,* ataupun virus melalui tautan. Selain itu, modus kejahatan ini juga memanfaatkan psikologis pengguna dengan menciptakan situasi darurat yang menyerang kerabat atau orang terdekat. Sehingga pelaku kejahatan siber dengan mudah memperoleh data pribadi pengguna.

Privasi Data

Risiko yang berhubungan privasi data juga menjadi risiko tidak hanya bagi perorangan tetapi perusahaan dan lembaga pemerintah yang menyimpan sejumlah besar data penting, seperti alamat rumah atau nomor telepon.

[11] Duanaiko, Anaq; Haryanto, Janitra, Darmawan, Paska; Khong, Yuliana. (2019). Kompetensi Keamanan Teknologi Digital di Indonesia: Analisis Fenomena Penipuan dengan Teknik Rekayasa Sosial. White Paper Kerjasama Center for Digital Society dan Gopay Indonesia

Privasi data mengacu pada cabang keamanan yang berfokus pada cara melindungi informasi ini dan menjauhkannya dari peretas dan penjahat dunia maya. Ada beberapa penyebab paling umum dalam kasus pembobolan data, yaitu kata sandi/kredensial yang lemah dan mudah dicuri, *back door* dan kerentanan aplikasi, perangkat lunak yang berbahaya, *social engineering*, terlalu banyak izin mengakses data, ancaman orang dalam, kesalahan konfigurasi, dan kesalahan pengguna.

Modus OTP *(One-Time Password)*

Di akhir tahun 2019, kasus baru muncul dengan menggunakan fitur *call forwarding* untuk mendapatkan kode OTP *(one-time password)* dari pengguna platform digital. Lagi-lagi pelaku kejahatan beroperasi dengan hanya menciptakan suasana yang meyakinkan bagi para korban, dan bukan memanfaatkan celah dari segi sistem/platform. Oleh karenanya, pemilik akun/pengguna merupakan pihak yang paling penting dalam upaya penyelesaian rantai keamanan siber.[12]

Terlebih selama masa pandemi, tercatat bahwa modus kejahatan siber seringkali memanfaatkan *fear mongering* pengguna, dimana, pada masa seperti sekarang ini, pengguna kerap memiliki rasa ingin tahu dan kepanikan terkait isu ataupun berita yang berkaitan dengan COVID-19.

Peretas juga memanfaatkan keluguan pengguna baru khususnya UMKM baru yang mengalami kenaikan yang signifikan selama pandemi. Selama kuartal pertama 2020 masa pandemi, Kaspersky menemukan 192,591 serangan *phishing* terhadap UMKM. Kasus ini meningkat dari 158,492 pada kuartal pertama 2019.[13]

Selain menyasar UMKM, serangan *phishing* selama masa pandemi memanfaatkan tingginya kebutuhan masyarakat indonesia akan *entertainment* selama di rumah dan belanja daring. Sehingga peretasan turut menyasar pengguna *e-commerce* yang mengakibatkan kebobolan data dan maraknya modus penipuan layanan *streaming* berbayar dengan iming-iming gratis.[14]

Pretexting

Selama masa pandemi, tercatat juga beberapa kasus dengan modus lama seperti *pretexting*, yang memanfaatkan tingginya keikutsertaan masyarakat dengan kuis berhadiah *giveaway* dari publik figur.[15] Motivasi masyarakat terhadap investasi berbunga tinggi selama pandemi juga kerap dimanfaatkan oleh para peretas yang mengatasnamakan *e-commerce* dan platform investasi saham untuk mendapatkan data pribadi pengguna.[16]

[12] Op.cit. Duanaiko, Anaq; Haryanto, Janitra, Darmawan, Paska; Khong, Yuliana. (2019).

[13] Annur, Cindy Mutia. (2020). UKM Indonesia Jadi Target 192 Ribu Serangan Siber Selama WFH, [daring]. Tersedia di: https://katadata.co.id/happyfajrian/digital/5eb923b47a779/ukm-indonesia-jadi-target-192-ribu-serangan-siber-selama-wfh. (diakses pada: Oktober 2020)

[14] Burhan, Fahmi Ahmad. (2020). Efek Pandemi, 700 Lebih Situs Netflix dan Disney Plus Palsu Curi Data, [daring]. Tersedia di: https://katadata.co.id/desysetyowati/digital/5e9d25848737e/efek-pandemi-700-lebih-situs-netflix-dan-disney-palsu-curi-data. (diakses pada: Oktober 2020)

[15] Salim, Hanz Jimenez. (2020). Waspada Akun Palsu Baim Wong hingga Soimah Bagi-Bagi Hadiah di Facebook. (daring). Tersedia di: https://www.liputan6.com/cek-fakta/read/4350502/waspada-akun-palsu-baim-wong-hingga-soimah-bagi-bagi-hadiah-di-facebook . (diakses pada: Oktober 2020)

[16] Investor Daily. (2020). Waspadai Modus Penipuan Baru Dalam Investasi Saham. (daring). Tersedia di: https://investor.id/market-and-corporate/waspadai-modus-penipuan-baru-dalam-investasi-saham. (diakses pada: Oktober 2020)

Deep fakes

Deep fakes juga akan mendominasi risiko dari tren siber di dunia. *Deep Fakes* adalah kombinasi dari kata "*deep learning*" dan "*fake*". *Deep Fakes* terjadi ketika teknologi kecerdasan buatan *(Artificial Intelligence/AI)* dapat menghasilkan gambar dan suara palsu yang tampak nyata. *Deep fakes* memungkinkan untuk memanipulasi gambar atau video dari seseorang untuk menggambarkan beberapa aktivitas yang sebenarnya tidak terjadi. Berada di tangan yang salah, *deep fakes* dapat digunakan untuk menciptakan *hoax* yang melibatkan tokoh penting, termasuk politisi dan selebriti.

Penggunaan *deep fakes* untuk serangan siber masih jarang terjadi di Indonesia. Menurut Field Chief Security Officer Asia Pacific Palo Alto Networks Kevin O'Leary pada akhir tahun 2019, teknologi ini memang belum muncul di wilayah Asia Tenggara, karena teknologi ini masih dalam tahap pengembangan.[17]

Namun demikian, video yang sempat diunggah oleh komedian Jordan Peele dan menjadi perbincangan di Amerika Serikat menunjukkan bahwa teknologi tersebut mampu membuat video palsu menjadi terlihat sangat asli. Kemampuan *deep fakes* yang telah didemonstrasikan dalam video tersebut menunjukkan bahwa, di masa depan, *deep fakes* sangat mungkin digunakan sebagai disinformasi terhadap seseorang maupun entitas tertentu. Meski *digital watermark* dapat menjadi alat untuk memverifikasi *deep fakes* tersebut, verifikasi tidak serta merta memampukan penerima informasi menolak untuk memercayai informasi palsu tersebut.

Modus operandi serangan siber berkembang mengikuti kecepatan teknologi, dan mengeksploitasi kerapuhan pengguna di platform digital, digabungkan dengan teknik *social engineering*.[18]

Seiring dengan perkembangan teknologi dan perubahan perilaku pengguna digital, misalnya pengguna yang beralih dari SMS ke aplikasi pesan, banyaknya pengguna yang beralih dari pembayaran tunai menjadi cashless, atau semakin tergantungnya masyarakat terhadap platform digital selama pandemi, membuat pelaku kejahatan siber turut mengubah sasaran platform serangan siber.

Sistem keamanan teknologi digital merupakan faktor penting dalam memastikan keamanan ekosistem digital. Namun, beberapa contoh serangan siber tersebut menunjukkan bahwa psikologis manusia masih menjadi titik lemah target serangan. Karena itu diperlukan kerjasama semua pihak untuk membuat internet lebih aman.

[17] Hafis, Faisal. (2019). Pakar AS: Cepat atau Lambat, Indonesia akan Hadapi Deepfake. Cyberthreat.id, [daring). Tersedia di : https://cyberthreat.id/read/4118/Pakar-AS-Cepat-atau-Lambat-Indonesia-akan-Hadapi-Deepfake. (diakses pada: September 2020)

[18] Op.cit. Duanaiko, Anaq; Haryanto, Janitra, Darmawan, Paska; Khong, Yuliana. (2019).

3 MENDORONG TRANSPARANSI KEAMANAN SIBER PERUSAHAAN

Seiring dengan perpindahan hampir semua kegiatan masyarakat dari ranah luring ke ranah daring, keamanan platform digital menjadi hal yang krusial. Hal ini disebabkan oleh besarnya data pribadi yang pengguna berikan kepada platform digital.

Data pribadi merupakan aset penting di era digital. Dari sisi penyedia produk dan layanan digital, data pribadi dibutuhkan oleh industri untuk memaksimalkan kualitas produk dan meningkatkan kemudahan penggunanya. Sementara di sisi lain, para pelaku serangan siber juta memahami pentingnya data tersebut. itulah sebabnya segala serangan, mulai dari *ransomware* hingga *phishing*, terus meningkat.

Seiring dengan semakin banyaknya perangkat digital yang terhubung dengan kehidupan masyarakat, semakin tinggi pula risiko keamanan individu di ranah digital. Maka dari itu, individu perlu merasa yakin bahwa data pribadi yang mereka berikan kepada perusahaan itu aman, dan layanan digital yang mereka gunakan dapat dipercaya, serta diandalkan. Sayangnya, masih banyak perusahaan yang tidak melaporkan strategi mitigasi ancaman siber tersebut.

Berdasarkan riset dari PwC[19] terhadap para CEO di beberapa negara, terungkap bahwa mereka melihat serangan siber sebagai ancaman yang semakin meningkat. Masih dari laporan yang sama, investor juga melihat serangan siber sebagai ancaman terbesar bagi perusahaan tempat di mana mereka memiliki saham.

Adanya serangan siber juga dapat menghilangkan kepercayaan konsumen terhadap kapasitas perusahaan dalam menjaga dan melindungi data pribadi mereka.

Di satu sisi, dapat dimaklumi apabila terdapat kekhawatiran dari perusahaan untuk membeberkan sistem keamanan siber mereka secara detail kepada masyarakat umum. Hal ini dikarenakan informasi yang tersebar justru dapat dimanfaatkan oleh pelaku serangan siber untuk dengan mudah mencari celah sistem tersebut.

Namun di sisi lain, untuk mendapatkan kepercayaan dari konsumen, regulator, dan masyarakat luas lainnya, perusahaan tetap perlu bersikap terbuka mengenai kebijakan dan standar praktik keamanan siber mereka.

Perusahaan berkesempatan untuk tidak hanya meyakinkan pemangku kepentingan, tapi juga memainkan peran konstruktif ke dalam komunitas digital yang lebih aman.

Untuk mencapai ini, perusahaan bisa dan perlu melaporkan secara detail tentang tata kelola keamanan siber mereka; struktur dan kapabilitas apa yang diterapkan untuk mengatur risiko.

Salah satu praktik membangun transparansi yang menarik disimak adalah yang dilakukan TikTok. Dalam hal penyimpanan data, setiap pusat data TikTok memiliki pertahanan dan keamanan fisik serta jaringan yang canggih. Semua data pengguna TikTok disimpan di luar negara Tiongkok.

Selain itu, di tahun ini TikTok juga membuka Pusat Transparansi dan Akuntabilitas TikTok di Los Angeles dan Washington DC dimana di kedua tempat ini, para pemangku kepentingan dapat melihat sendiri praktik keamanan dan infrastruktur dari TikTok, terutama mencakup program pertahanan siber, jaminan keamanan serta perlindungan data TikTok.

[19] PwC Report (2018). Transparency in the Digital Age: Companies should talk about their cyber security, [daring]. Tersedia di: https://www.pwc.co.uk/cyber-security/pdf/transparency-in-the-digital-age.pdf. (diakses pada: Oktober 2020)

4 MEMBERDAYAKAN PENGGUNA PLATFORM

Dengan melihat berbagai macam kasus serangan siber yang terjadi di Indonesia, kajian ini melihat bagaimana literasi digital merupakan salah satu upaya penting untuk memberdayakan masyarakat digital di Indonesia. Banyaknya kasus serangan siber tersebut mengindikasikan rendahnya tingkat literasi digital dari pengguna, khususnya dalam mengatasi ancaman siber.

Penelitian CfDS dalam Kajian Peningkatan Kompetensi Keamanan Digital di Indonesia, memaparkan tipologi literasi berdasarkan tiga kategori: dasar *(basic)*, menengah *(intermediate)*, dan lanjutan *(advanced)*.

Dasar *(Basic)*

- Mengetahui cara memasang kata sandi
- Memahami cara berinteraksi / bertransaksi secara daring
- Mengetahui bahwa tidak semua informasi daring dapat dipercaya
- Menyadari adanya penipuan dengan teknik rekayasa sosial
- Mengetahui cara mengakses dan menggunakan OTP
- Tidak membagikan kata sandi akun kepada orang lain
- Menghindari penggunaan kata sandi yang mudah ditebak.

Menengah *(Intermediate)*

- Memasang metode pengamanan ganda bila disediakan
- Memasang *multi-factor authentification code* akun (metode pengamanan dengan jumlah lebih dari satu) seperti kata sandi atau cara otentikasi lain
- Tidak membagikan OTP kepada orang lain secara sadar
- Tidak membagikan nomor telepon alamat email, nama lengkap, dan nomor tanda pengenal identitas di media sosial secara publik
- Mengetahui cara mengakses informasi platform mengenai perangkat yang sedang mengakses akun tersebut bila disediakan
- Menggunakan kata sandi berbeda beda pada tiap akun digital
- Mengganti kata sandi secara berkala
- Melakukan log-out akun platform bila tidak digunakan.

Lanjutan *(Advanced)*

- Mengetahui perintah-perintah yang tidak umum dalam penggunaan telepon genggam (seperti : *call-forwarding*)
- Memperbaharui pengetahuan mengenai modus penipuan dengan teknik rekayasa sosial secara rutin
- Memperbaharui pengetahuan mengenai cara melindungi diri dari penipuan dengan teknik rekayasa sosial secara rutin.

Tabel 1. Kompetensi Keamanan Teknologi Digital (KKTD)[20]

[20] Op.cit. Duanaiko, Anaq; Haryanto, Janitra, Darmawan, Paska; Khong, Yuliana. (2019).

Dengan mengacu pada tingkat kompetensi keamanan teknologi digital tersebut dan tingginya jumlah kasus serangan siber di Indonesia, dapat disimpulkan bahwa tingkat kompetensi pengguna teknologi di Indonesia masih berada pada tingkat dasar *(basic)* dan menengah *(intermediate)*[21]. Jumlah kasus laporan yang terjadi mengisyaratkan bahwa korban belum memahami atau memiliki kemampuan literasi digital yang mumpuni. Khususnya untuk terhindar dari ancaman tindak kejahatan tersebut.

Pemberdayaan dari tingkat pengguna dapat dilakukan dengan meningkatkan kompetensi dasar. Pengguna diharapkan untuk bisa meningkatkan kompetensi dari diri sendiri dengan cara mengganti kata sandi *(password)* akun pribadi secara berkala, membatasi penggunaan *Wi-Fi* publik ketika sedang melakukan transaksi digital yang hubungannya dengan data pribadi, meneliti reputasi keamanan platform yang ingin digunakan, ataupun membuat perlindungan autentifikasi khusus akun dengan menghubungkannya pada email/nomor HP pengguna.[22]

Pengguna yang telah melampaui kompetensi tingkat dasar dapat terus meningkatkan pengetahuan mengenai kasus keamanan siber dengan memperbaharui pengetahuan melalui berita/media terkait kasus keamanan siber dan selalu belajar dari metode serangan siber agar terhindar dari upaya kejahatan.[23]

Peran Pengguna dalam Menciptakan Keamanan Komunitas Digital

Selain dari sisi keamanan platform, pengguna layanan digital merupakan aktor terdepan dalam upaya membangun komunitas digital yang aman dari serangan siber. Perilaku pengguna dalam berinteraksi dan bertransaksi di dunia digital menjadi salah satu faktor pendukung terbesar dari ekosistem digital yang bebas ancaman. Tingkat kesadaran pengguna akan keamanan digital dari dalam diri ini secara langsung akan berimplikasi pada kesadaran kelompok, dan juga kesadaran pemilik platform untuk membangun pelayanan yang aman dari ancaman siber.

Oleh karenanya, pengguna diharapkan untuk memastikan beberapa faktor penting sebelum memanfaatkan layanan di platform digital:

1. Pilih platform yang menunjukkan komitmennya dalam menjaga keamanan digital pengguna

Cara termudah untuk tetap aman di dalam komunitas digital adalah dengan berperilaku selektif terhadap platform sebagai pemberi layanan. Pengguna dapat memilih platform yang memiliki komitmen untuk melindungi pengguna dari ancaman siber, dengan memastikan ketersediaan pusat layanan keamanan *(Safety Center)* pada platform.

Pusat layanan keamanan ini akan memberikan panduan dan informasi yang diperlukan mengenai langkah yang diambil oleh platform tersebut untuk memastikan keamanan pengguna, seperti yang terdapat di platform[24] TikTok.

[21] Lampiran

[22] Op.cit. Duanaiko, Anaq; Haryanto, Janitra, Darmawan, Paska; Khong, Yuliana. (2019).

[23] ibid

[24] TikTok (2020). Transparency Report, [daring]. Tersedia di: https://newsroom.tiktok.com/safety/resources/transparency-report-2020-1?lang=id. (diakses pada: Oktober 2020)

2. Perhatikan data apa saja yang diminta platform *(data collection)*

Pada saat membuka akun suatu platform, pengguna akan diminta untuk memasukkan beberapa data pribadi, seperti nama lengkap, tanggal lahir, jenis kelamin, dan lokasi. Dengan adanya risiko penyalahgunaan data, pengguna perlu menaruh perhatian terhadap data yang ia berikan kepada platform tersebut - apakah masih dalam batas wajar atau sudah terlalu rahasia, seperti meminta nomor PIN kartu kredit dan lainnya.

TikTok memiliki komitmen dalam menjaga privasi data dari pengguna. Karena itu TikTok selalu transparan dalam mengumpulkan informasi dari penggunanya. Untuk meningkatkan pengalaman pengguna dalam platform, mengembangkan produk dan fitur yang lebih baik serta memberikan rekomendasi konten dan iklan yang relevan kepada pengguna, TikTok mengumpulkan beberapa informasi antara lain seperti sistem informasi, jejak rekam di platform TikTok, informasi ketika membuka akun.

3. Pastikan platform memiliki panduan komunitas *(Community Guidelines)*

Untuk menjaga keamanan bersama seluruh pengguna, selalu pastikan ketersediaan panduan komunitas *(Community Guidelines)* dalam platform. Hal ini perlu dilakukan untuk menjaga komunitas yang selalu positif dan kreatif, serta terhindar dari individu/organisasi berbahaya, *scam*/penipuan digital, peretasan data pribadi, dan lainnya.

Panduan Komunitas berfungsi sebagai pedoman mengenai konten apa yang boleh dan tidak boleh diunggah ke dalam aplikasi atau platform, dan kebijakan di dalamnya akan selalu diperbaharui untuk disesuaikan dengan kondisi yang sedang terjadi di masing-masing negara. Platform TikTok kerap mensosialisasikan Panduan Komunitas[25] dalam setiap kegiatannya, dengan tujuan pengguna lebih bertanggung jawab untuk menjaga lingkungan platform tetap aman dan nyaman bagi semua pengguna.

TikTok juga rutin mempublikasikan Laporan Transparansi untuk menyediakan wawasan mengenai jumlah konten dan alasan mengapa konten tersebut dihapus. Selain pelanggaran Panduan Komunitas atau Ketentuan Layanan, Laporan Transparansi ini juga mencakup bagaimana TikTok merespon terhadap permintaan informasi yang diajukan lembaga penegak hukum, permohonan penghapusan konten oleh pemerintah, dan laporan terhadap konten yang dianggap melanggar hak cipta.

[25] TikTok (2020). Panduan Komunitas, [daring]. Tersedia di: https://www.tiktok.com/community-guidelines?lang=id. (diakses pada: Oktober 2020)

4. Pastikan komitmen platform untuk menyediakan transparansi bagi keamanan bersama

Platform yang berkomitmen untuk melindungi pengguna dari ancaman siber akan selalu berupaya untuk terlibat dalam membangun komunitas yang sehat dan terlindung. Salah satu cirinya adalah platform akan secara proaktif menghadirkan transparansi dalam menjaga keamanan penggunanya.

Seperti contoh Pusat Transparansi dan Akuntabilitas TikTok di Amerika Serikat yang diharapkan dapat menjadi tempat bagi dialog bermakna bagi pemangku kepentingan dalam membantu TikTok mengembangkan kebijakan yang terkait dengan keamanan dan kenyamanan pengguna.

5. Pastikan kepemilikan kontrol pengguna terhadap akun pribadinya *(You're in Control!)*

Untuk tetap menjaga keamanan dalam memanfaatkan layanan/pengalaman di dunia digital, selalu pastikan hak atas akun pengguna. Platform yang aman akan mengizinkan pengguna untuk memiliki kontrol dalam mengatur akun pribadinya, preferensi konten, maupun jejaring sosial pribadi dalam penggunaan layanan tersebut.

Kebebasan pengguna dalam mengatur akunnya ini bisa meliputi banyak hal, mulai dari siapa yang bisa melihat kontennya atau berkomentar, menyaring kata kunci yang sensitif, serta bisa melaporkan konten lain yang dianggap berbahaya. Hal inilah yang dipastikan oleh TikTok melalui fitur *'Manage My Account'*.

Bukan hanya itu, pengguna memiliki kebebasan untuk meminta akses atau menghapus informasi yang sudah dibagikan ke TikTok, menolak atau mematikan *cookies*, atau mengatur preferensi iklan yang lewat di lamannya.

Lapisan keamanan TikTok lainnya adalah *Family Pairing* atau Pelibatan Keluarga, yang memungkinkan akun orangtua untuk terkoneksi dengan akun anak remajanya, sehingga orang tua dapat ikut berperan untuk mengontrol akun anaknya agar tetap aman dan nyaman dalam menggunakan TikTok.

5

PENTINGNYA KERJASAMA PEMANGKU KEPENTINGAN

Kajian ini melihat bahwa kolaborasi antar pemangku kepentingan merupakan salah satu langkah efektif, dikarenakan tiap sektor dapat memberikan sumbangsih dan peran serta dalam menangani ragam permasalahan digital di Indonesia.

Secara umum, pemerintah sebagai institusi yang mendapatkan legitimasi dari masyarakat untuk menjaga keteraturan sosial dan menjaga keamanan dan kenyamanan masyarakat memiliki kewajiban untuk menyusun dan menetapkan kebijakan yang berorientasi pada keamanan dan kenyamanan pengguna.

Sementara itu, pelaku industri harus berupaya dalam melindungi pengguna dengan terus meningkatkan inovasi keamanan, melindungi data pribadi dan melakukan langkah edukasi untuk meningkatkan resiliensi pengguna.

Kajian ini merekomendasikan sinergi para aktor secara holistik dengan peran dan kapabilitas masing-masing aktor yaitu industri, akademisi, pemerintah, komunitas dan pengguna sendiri dalam meningkatkan resiliensi dan mencegah serangan siber.

Secara detail masing-masing pemangku kepentingan memiliki peranan sebagai berikut :

Tabel 2. Peranan masing-masing pemangku kepentingan dalam menciptakan keamanan digital (diolah oleh penulis)[26] [27] [28]

INDUSTRI	- Transparan dengan pengumpulan dan kontrol terhadap data pengguna - Menciptakan ekosistem keamanan data yang baik - Terlibat aktif dalam peningkatan kesadaran pengguna terkait data pribadi - Secara konsisten mengadakan kampanye edukasi, kajian dan inovasi fitur platform yang inklusif - Melakukan kajian dan inovasi fitur platform yang inklusif sesuai dengan target sasaran pengguna - Memberikan rekomendasi dan masukan khususnya kepada Pemerintah dan Akademisi berdasarkan kebutuhan pengguna dan kebutuhan industri masa depan.
PEMERINTAH & REGULATOR	- Menindak pelanggaran hukum terkait dengan kasus keamanan siber - Meminimalisir penyalahgunaan data, baik yang dikumpulkan, disimpan, dan diproses oleh pemerintah atau oleh pihak-pihak lainnya - Menampung masukan industri dalam merumuskan kebijakan terkait perlindungan data pengguna.

[26] Naresh K. Malhotra, Sung S. Kim, and James Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research 15, no. 4 (2004): pp. 336-355, https://doi.org/10.1287/isre.1040.0032.

[27] Op.cit. Duanaiko, Anaq; Haryanto, Janitra, Darmawan, Paska; Khong, Yuliana. (2019).

[28] Rahman, Faiz & Anggika Rahmadiani. (2019). Perlindungan Data Pribadi di Indonesia: perspektif Hukum dan Sosial. Digitimes. CfDS

 KOMUNITAS DAN ORGANISASI MASYARAKAT	- Secara umum, komunitas dan ormas yang berada di tengah masyarakat dapat memberikan edukasi publik *watchdog* dan berkontribusi pada analisis kebijakan sesuai dengan kebutuhan masyarakat - Organisasi masyarakat seperti Siberkreasi, ICT Watch, Relawan TIK Indonesia harus terus memberikan edukasi untuk meningkatkan resiliensi pengguna kaitannya dengan literasi digital - Organisasi masyarakat seperti SAFEnet dan ELSAM (Lembaga Studi dan Advokasi Masyarakat), PARFI (Persatuan Artis Film Indonesia), Indonesia Internet Governance Forum, Jaringan Pegiat Literasi Digital Indonesia, Siberkreasi maupun Lembaga Keamanan Konsumen (contoh: YLKI) diharapkan dapat meningkatkan kesadaran pengguna kaitannya dengan isu keamanan data pribadi.
 AKADEMISI	- Menyiapkan Sumber Daya Manusia (SDM) yang kompeten, khususnya yang memiliki kecakapan dalam bidang keamanan siber - Melakukan kajian peningkatan kemampuan literasi digital dan memperbaharui data terkait dengan ancaman siber khususnya di Indonesia - Melakukan penelitian yang dapat mendorong inovasi teknologi, sekaligus memberikan rekomendasi bagi industri - Melakukan evaluasi kebijakan dan input rekomendasi bagi pemerintah dan regulator.
 PENGGUNA	- Memiliki pengertian bahwa data dapat dikontrol oleh masing-masing individu, sehingga waspada dengan keamanan data pribadi - Tidak menggunakan satu email untuk berbagai platform - Melakukan penggantian kata sandi secara berkala - Membuat kata sandi yang rumit dan unik (bila perlu gunakan manajemen kata sandi) - Mengaktifkan otentikasi dua faktor - Aktif mencari informasi terkait keamanan data untuk meningkatkan resiliensi atas data pribadi - Terus memperbaharui informasi mengenai isu terkait keamanan siber - Turut membantu industri atau platform dalam melaporkan konten yang tidak pantas atau yang tidak aman.

Selain memiliki tugas dan peran untuk masing-masing pemegang kepentingan, diperlukan pula strategi dan pengambilan langkah untuk mewujudkan transparansi dalam keamanan siber.

Beberapa langkah yang perlu diperhatikan, antara lain:

Kepemimpinan dan Regulasi

Faktor kepemimpinan yang selama ini diemban oleh pemerintah Indonesia menjadi kunci dalam peningkatan keamanan siber di Indonesia. Terdapat dua hal penting yang dapat diupayakan oleh pemerintah dalam menjamin keamanan siber di Indonesia.

Pertama, pemerintah harus dapat menjadi percontohan dalam transformasi digital, utamanya di dalam organisasinya sendiri. Hal ini menjadi penting karena pemerintah harus dapat menjadi percontohan bagi masyarakat dan sektor swasta dalam transformasi digital yang progresif. Karenanya, strategi transformasi digital ini dapat dimulai dari dalam organisasi pemerintah sendiri.

Strategi digitalisasi di dalam organisasi pemerintah dapat mempertimbangkan beberapa faktor, di antaranya[29] :

- Persamaan visi dari seluruh anggota organisasi pemerintah bahwa transformasi digital sangatlah diperlukan saat ini
- Kepemimpinan digital, yaitu pemimpin pemimpin organisasi yang memahami pentingnya digitalisasi di dalam organisasinya dan memiliki kemampuan untuk memberikan arahan
- Sumber daya manusia yang memiliki keterampilan digital sesuai dengan fungsinya
- Infrastruktur TIK yang mendukung transformasi digital, pola pikir digital yang mendorong kolaborasi dalam digitalisasi
- Budaya kerja yang mampu beradaptasi dengan cepatnya perkembangan teknologi
- Model bisnis yang mengadopsi teknologi- teknologi digital dan dijalankan dengan digital mindset
- Ambisi digital, yang didukung bersama oleh seluruh lapisan organisasi pemerintah

Apabila pemerintah Indonesia telah dapat menjadi percontohan dalam transformasi digital, maka akan dapat menjalankan fungsi kepemimpinan dan regulasi dengan lebih baik.

[29] Venter. 2018. The Influence of digital transformation on leadership in state-owned enterprises. Gordon Institute Business Scholl,University of Pretoria. (online). Tersedia di : https://repository.up.ac.za/bitstream/handle/2263/68818/Venter_Influence_2018.pdf?sequence=1. (diakses pada: Oktober 2020)

Kedua, selama ini pemerintah Indonesia telah mengeluarkan kebijakan-kebijakan dan strategi nasional yang bertujuan untuk membentuk ekosistem digital yang inklusif dan aman. Pemerintah harus memastikan bahwa kebijakan-kebijakan dan strategi nasional tersebut senantiasa sesuai dengan perkembangan teknologi yang ada.

Regulasi yang dikeluarkan oleh pemerintah diharapkan mampu menjawab tantangan perkembangan teknologi yang sangat cepat dan bersifat disruptif, dan dapat memastikan bahwa tata kelola keamanan siber dan transformasi digital di Indonesia harus terintegrasi dengan baik dari satu kementerian/ lembaga dengan kementerian/ lembaga lainnya.

Selain itu, pemerintah pun perlu mengalokasikan anggaran dan sumber daya ahli untuk menerapkan strategi keamanan siber ini.

Analisa dan Manajemen Risiko

Serangan siber dapat terjadi kapan saja dan terus berkembang. Oleh karena itulah, diperlukan adanya kesiapan dan resiliensi. Pihak swasta dan publik perlu membangun kemampuan untuk merespon risiko potensial. Komunikasi antar pihak juga dipastikan tetap lancar untuk berbagi informasi yang dapat membantu terwujudnya keamanan siber.

Melalui pusat keamanannya, TikTok tidak hanya dapat memantau ancaman dunia siber yang akan datang tetapi juga merespon insiden kritis.

Selain itu, dalam Pusat Transparansi dan Akuntabilitas TikTok, pengunjung juga dapat meninjau strategi pertahanan berlapis yang antaranya meliputi pertahanan lapisan jaringan dan tim manajemen kerentanan global.

Pembangunan Kapasitas dan Kesadaran

Untuk menjaga keamanan siber, diperlukan sumber daya yang juga memiliki kemampuan khusus. Berdasarkan laporan dari *Information System Security Association* di bulan Juli 2020[30], terdapat 82% petinggi perusahaan di seluruh dunia yang mengatakan kekurangan tenaga kerja yang memiliki kemampuan keamanan siber.

Ini menjadi momen yang tepat untuk memasukan kurikulum keamanan siber ke dalam sistem pendidikan serta mengadakan program dan badan riset untuk membentuk kemampuan keamanan siber ini.

Selain untuk mencetak sumber daya ahli yang dapat menangani masalah keamanan siber, diperlukan juga peningkatan literasi digital masyarakat Indonesia terhadap keamanan digital. Berdasarkan studi terkini, kemampuan dan pemahaman mengenai *digital safety* mahasiswa Indonesia yang paling rendah apabila dibandingkan dengan kemampuan dan pemahaman digital lainnya.[31]

Idealnya, jika pemberdayaan penggunaan dapat diintegrasikan ke dalam kurikulum informatika di sekolah, maka kemungkinan penguatan akan keamanan siber pengguna Indonesia dapat terjadi dengan masif.

[30] Information System Security Association (2020). The Life and Times of Cybersecurity Professionals 2020.

[31] Mantovani, Duanaiko, Haryanto, Angendari, & Putri. (2020). Higher Education 4.0 and the Readiness of Indonesia's Future Workforce. Yogyakarta : Center for Digital Society.

Kerjasama Internasional

Permasalahan keamanan siber terjadi di hampir semua negara, mengingat serangan siber dapat terjadi lintas negara. Sejumlah kasus memperlihatkan bagaimana serangan dilakukan oleh peretas yang berada di negara lain, dan karena itulah kerjasama antar negara itu penting. Diskusi dan inisiatif di tingkat internasional perlu digaungkan dan melibatkan berbagai negara guna terciptakan kolaborasi baik secara formal maupun informal untuk menciptakan keamanan siber di dunia.

Salah satu contoh kolaborasi antar negara ini terlihat dari pembentukan Dewan Penasihat Keamanan TikTok[32] yang dibentuk di tingkat wilayah Asia Pasifik, menyusul sebelumnya telah dibentuk pula Dewan Penasihat Konten Amerika Serikat di awal tahun ini. Dewan ini menyatukan pemimpin dari sektor akademis, hukum, dan pemerintah dari berbagai negara di wilayah Asia Pasifik, yang bertugas menyediakan anjuran berdasarkan keahliannya tentang kebijakan dan praktik moderasi konten di TikTok, agar dapat membantu pembentukan panduan global dan regional.

Dewan ini akan mendukung TikTok dalam mengembangkan kebijakan kedepannya. Kebijakan ini tidak hanya menjawab tantangan masa kini, tapi juga mengidentifikasi permasalahan yang ada dan sedang berkembang di Asia Pasifik, yang dapat mempengaruhi platform serta pengguna TikTok.

[32] TikTok (2020). Memperkenalkan Dewan Penasihat Keamanan Asia Pasifik TikTok, [daring]. Tersedia di: https://newsroom.tiktok.com/in-id/memperkenalkan-dewan-penasihat-keamanan-asia-pasifik-tiktok. (diakses pada: Oktober 2020)

6 KESIMPULAN

Keamanan siber baik untuk sektor publik maupun sektor swasta merupakan isu yang semakin meningkat di masyarakat, terutama selama pandemi dimana semakin banyak individu dan perusahaan yang saling bergantung kepada perangkat dan internet. Perpindahan aktivitas luring menjadi daring adalah suatu keniscayaan bahkan setelah pandemi berakhir, sehingga kolaborasi berbagai pemangku kepentingan untuk menentukan suatu strategi dan mempercepat literasi digital, menjadi suatu keharusan.

Beberapa poin yang menjadi rekomendasi dari kajian ini, antara lain:

1. Pemerintah melanjutkan kepemimpinan dalam proses transformasi digital, pembuat peraturan yang bersinergi dengan lembaga lainnya, dan pengalokasian anggaran untuk peningkatan sumber daya.
2. Perlunya transparansi di tingkat perusahaan mengenai kebijakan dan praktik keamanan siber demi memberikan keyakinan dan ketenangan kepada seluruh pemangku kepentingan.
3. Peningkatan sumber daya manusia melalui riset dan pembangunan, serta percepatan literasi digital untuk memberdayakan pengguna mengenai keamanan digital.
4. Kolaborasi dengan berbagai pihak untuk bersama-sama menjaga keamanan dunia siber.

TikTok, sebuah platform yang dibangun dengan misi untuk menginspirasi kreativitas dan membawa kebahagiaan berkomitmen penuh mendukung pengguna kami untuk merayakan hal yang membuat mereka unik. Rasa aman tentu membantu banyak orang merasa nyaman mengekspresikan diri secara terbuka, yang membuat kreativitas makin berkembang.

Melalui kajian ini, kami mengajak pemangku kepentingan dan tentunya pemerintah untuk bersinergi, bekerja bersama dalam upaya memperkuat keamanan data di Indonesia untuk ekosistem digital lintas sektor yang baik dan aman.

DISCLAIMER

Dokumen ini dibuat hanya untuk keperluan informasi Anda. Dokumen ini tidak membentuk rekomendasi oleh TikTok Pte. Ltd. ("Perusahaan") atau afiliasinya manapun (bersama-sama dengan Perusahaan disebut sebagai "TikTok") atau afiliasil, direktur, supervisor, officer, karyawan, agen, penasihat atau perwakilan yang mana pun dari masing-masing afiliasi atau Perusahaan (secara bersama-sama disebut sebagai "Perwakilan TikTok").

Walaupun kehati-hatian telah diterapkan untuk memastikan bahwa fakta yang disajikan dalam dokumen ini adalah akurat, dan opini yang dinyatakan adalah adil dan wajar, konten dari dokumen ini tidak terverifikasi secara terpisah. Dokumen ini berisi tautan ke situs atau sumber lain yang disediakan oleh pihak ketiga, yang mana tautan-tautan ini disediakan untuk keperluan informasi Anda saja. Kami tidak memiliki kontrol atas konten dari tautan atau sumber tersebut. Tautan tersebut tidak boleh diinterpretasikan sebagai persetujuan dari kami atas situs dengan tautan tersebut atau pun atas informasi yang Anda bisa dapatkan dari sana. Baik TikTok maupun Perwakilan TikTok tidak berada dalam kewajiban ataupun memberikan janji untuk menyediakan penerima akses terhadap infomasi tambahan atau untuk memperbaharui dokumen ini atau informasi tambahan lainnya atau untuk membenarkan informasi yang tidak akurat di dalamnya yang terlihat, dan baik TikTok maupun Perwakilan TikTok memiliki, hak, tanpa memberi alasannya, kapanpun, dan sehubungan dengan, perubahan atau amendemen informasi dalam dokumen ini atau pengakhiran proposal yang dideskripsikan dalam dokumen ini.

Tidak ada pernyataan atau jaminan, yang dinyatakan secara jelas maupun implisit, yang diberikan sebagai pencapaian atau kewajaran atas, dan tidak boleh ada ketergantungan yang ditempatkan pada, proyeksi, opini, estimasi, perkiraan, target, prospek, pendapatan atau pernyataan yang dicari lebih lanjut yang terdapat di dokumen ini. Proyeksi, estimasi, perkiraan, target, prospek, pendapatan atau pernyataan yang dicari lebih lanjut tersebut bukan merupakan indikator yang dapat diandalkan atas kinerja di masa mendatang. Baik TikTok maupun Perwakilan TikTok tidak bertanggung jawab atas konten di dalamnya, atas keakuratan, kelengkapan atau kecukupan dokumen ini atau atas informasi tertulis maupun lisan yang tersedia untuk pihak yang berkepentingan atau pun penasihatnya dalam hal apapun. Baik TikTok maupun Perwakilan TikTok tidak menyetujui untuk tanggung jawab atas kerugian yang timbul dari penggunaan atau pengandalan atas dokumen ini atau konten atau apapun yang timbul sehubungan dari hal tersebut.

Seluruh konten, gambar, teks, grafik, ilustrasi, logo, merk dagang, tanda layanan, hak cipta dan fotografi di sini dan seluruh hak kekayaan intelektual sehubungan dengan hal tersebut ("Konten TikTok") adalah milik atau dilisensikan kepada TikTok. Tidak ada dalam dokumen ini yang memberikan Anda hak kekayaan intelektual atau hak lainnya sehubungan dengan Konten TikTok. Konten TikTok tidak dapat diunduh, disalin, diproduksi ulang, didistribusikan, ditransmisikan, disiarkan, ditampilkan, dijual, dilisensikan atau diekspotasi untuk tujuan apapun tanpa persetujuan tertulis dari kami ataupun lisensor kami. Kami dan lisensor kami memiliki hak yang tidak tidak secara eksplisit diungkapkan di sini terhadap Konten TikTok.

TIM PENULIS

Tentang Center for Digital Society (CfDS)
Center for Digital Society (CfDS) adalah pusat studi yang didirikan oleh Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Gadjah Mada. Pusat studi ini berkomitmen untuk menghadirkan kajian dan informasi kepada masyarakat luas dan juga pemangku kepentingan di Indonesia mengenai isu digital strategis sebagai salah satu upaya untuk mewujudkan masyarakat digital yang inovatif, produktif dan berpengaruh di Indonesia.

Tentang Onno Center
Didorong oleh keinginan untuk berbagi pengetahuan dan berkontribusi dalam memberdayakan pendidikan di Indonesia, sejumlah praktisi Komunikasi dan Teknologi Informasi sepakat untuk membentuk yayasan bernama Yayasan Onno Center International yang fokus pada pendidikan Komunikasi dan Teknologi Informasi.