BADAN KEAHLIAN DPR RI

Pusat Analisis Anggaran dan Akuntabilitas Keuangan Negara

ANALISIS RINGKAS CEPAT 2024

EFEKTIVITAS PENGUATAN KEAMANAN SIBER DI INDONESIA

Pengarah : Dr. Inosentius Samsul, S.H., M.Hum.
Penanggungjawab : Dr. Ari Mulianta Ginting, S.E., M.S.E.
Penulis : Rendy Alvaro dan Achmad Yugo Pidhegso

www.bk.dpr.go.id

Analisis Ringkas Cepat: Efektivitas Penguatan Keamanan Siber di Indonesia

Summary

Pengelolaan anggaran terkait penguatan keamanan siber belum sepenuhnya efektif, hal ini dapat dilihat dari meningkatnya serangan siber di Indonesia dan masih relatif rendahnya indeks keamanan siber di Indonesia dibandingkan dengan jumlah pengguna internet di Indonesia. Kondisi tersebut diperparah dengan temuan audit BPK RI yang menunjukkan bahwa masih lemahnya koordinasi antar instansi terkait keamanan siber, kurangnya program peningkatan kompetensi SDM keamanan siber, dan program peningkatan awareness keamanan siber yang belum direncanakan dengan akurat.

PENDAHULUAN

Internet merupakan salah satu teknologi yang paling penting di era digital. Internet telah mengubah cara hidup dan bekerja orang-orang di seluruh dunia. Internet memungkinkan seluruh penggunanya untuk mendapatkan akses terhadap sumber informasi yang luas mulai dari berita, artikel, buku, hingga dokumentasi. Pengguna internet juga mendapatkan kemudahan dalam melakukan komunikasi karena internet memungkinkan manusia untuk berkomunikasi dengan orang lain di seluruh penjuru dunia dengan mudah dan murah. Bertumbuhnya pengguna internet di Indonesia tentunya perlu disertai dengan keamanan siber yang mumpuni. Herdiana, Munawar, dan Putri (2021) menjelaskan bahwa peralihan ke dunia digital tidak hanya terjadi pada interaksi sosial, bisnis, dan industri saja, namun juga diikuti dengan peralihan kejahatan ke dunia digital.

Data survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menyebutkan bahwa pengguna internet di Indonesia adalah terbanyak ke-4 di dunia pada tahun 2023 yaitu sebanyak 215.626.156 jiwa dibawah China, India, dan Amerika Serikat. Seluruh kegiatan masyarakat Indonesia dalam penggunaan internet pada aktivitas sehari-hari perlu untuk mendapatkan perlindungan khusus.

Pemerintah telah memiliki kebijakan terkait penguatan keamanan siber nasional yang dimuat dalam Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020–2024 yaitu dalam salah satu agenda pembangunan “Memperkuat Stabilitas Polhukhankam dan Transformasi Pelayanan Publik” dimana didalamnya terdapat Program Prioritas yaitu “Menjaga Stabilitas Keamanan Nasional” yang selanjutnya dijabarkan dalam lima kegiatan prioritas dengan semangat mengurangi serangan siber di Indonesia dan meningkatkan *Global Cybersecurity Index* (GCI).

Usaha penguatan keamanan siber di Indonesia dilaksanakan oleh beberapa instansi baik itu di pemerintah pusat dan pemerintah daerah yaitu antara lain pada Kementerian Komunikasi dan Informatika (Kemenkominfo), Kementerian Pertahanan (Kemenhan), Badan Siber dan Sandi Negara (BSSN), Badan Intelijen Negara (BIN), dan beberapa instansi lainnya. Namun, pada kenyataannya beberapa kasus terkait keamanan siber terjadi di Indonesia yaitu kasus peretas Bjorka, diretasnya data BPJS Kesehatan, dan diretasnya akun Youtube DPR RI. Melihat kenyataan tersebut, maka muncul pertanyaan, sudah efektif-kah penguatan keamanan siber di Indonesia? Pertanyaan tersebut dapat dijawab dengan menyajikan data serangan siber dan *Global Cybersecurity Index* di Indonesia, serta menjelaskan kondisi anggaran dan permasalahan dalam pelaksanaan anggaran terkait keamanan siber di instansi pemerintah.

PEMBAHASAN

Terjadi Tren Penurunan Anggaran Keamanan dan Ketahanan Siber

BSSN merupakan instansi yang memiliki tugas khusus di bidang keamanan dan ketahanan siber. Jika kita lihat dari sisi kemampuan untuk melakukan realisasi anggaran, BSSN secara umum mampu melakukan realisasi anggaran >95%, berikut merupakan data anggaran per program di BSSN:

Tabel 1. Anggaran per Program BSSN

Program	Anggaran & Realisasi	2018	2019	2020	2021	2022	Outlook 2023
Keamanan dan Ketahanan Siber dan Sandi Negara	Realisasi	689,66	2.001,04	515,88	785,40	150,20	216,40
	Anggaran	704,35	2.019,10	527,86	963,10	152,80	217,20
	%	97,91%	99,11%	97,73%	81,55%	98,30%	99,63%
Dukungan Manajemen	Realisasi	255,64	269,70	506,01	629,10	394,30	405,70
	Anggaran	264,91	289,00	534,09	963,10	401,80	407,10
	%	96,50%	93,32%	94,74%	65,32%	98,13%	99,66%

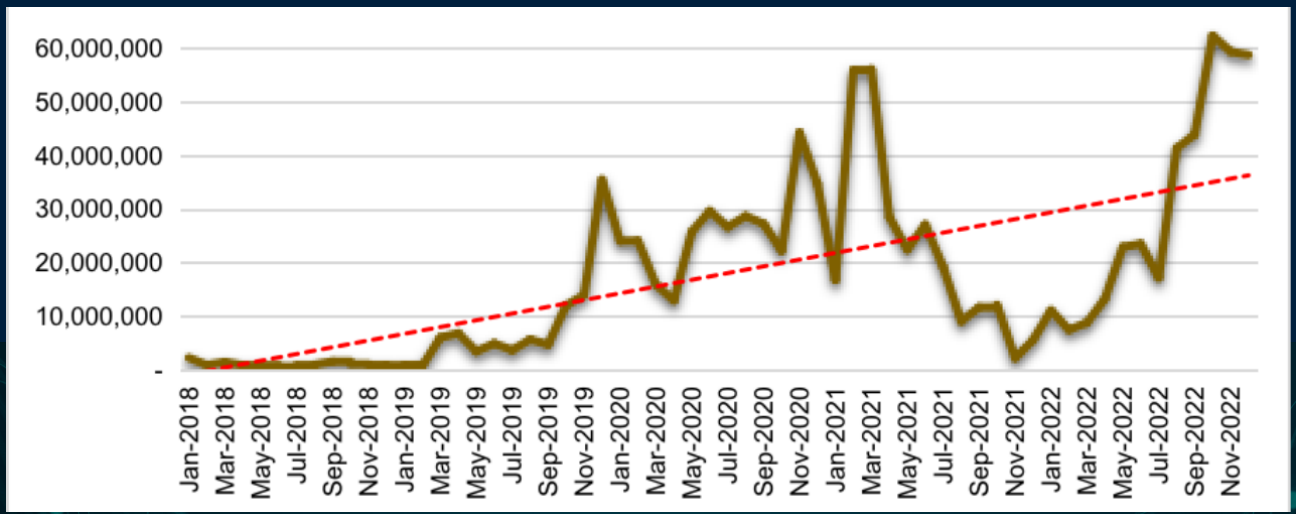
Sumber: Laporan Keuangan BSSN & Nota Keuangan APBN (2024)

Tabel 1 menunjukkan bahwa realisasi yang rendah hanya terjadi pada tahun anggaran 2021, namun dapat dilihat pada anggaran teknis terkait pengembangan keamanan dan ketahanan siber dan sandi negara terjadi tren penurunan. Hal ini berbanding terbalik dengan anggaran program dukungan manajemen. Tentunya hal ini menunjukkan ketidakseriusan pemerintah dalam hal penganggaran terkait keamanan siber.

Meningkatnya Serangan Siber di Indonesia

Terkait dengan ketercapaian tujuan, data BSSN menunjukkan bahwa serangan siber yang terjadi di Indonesia mengalami peningkatan signifikan, yaitu sebanyak 12.895.554 kasus pada tahun 2018 sedangkan pada tahun 2022 sebanyak 370.022.283 kasus, atau terjadi peningkatan 2.769% dari tahun 2018–2022, berikut merupakan data serangan siber:

Grafik 1. Serangan Siber di Indonesia Tahun 2018 - 2022



Sumber: Laporan Tahunan Honeynet Project BSSN – IHP Tahun 2018 – 2022, diolah (2024)

Grafik 1 menunjukkan bahwa semangat RPJMN 2020 – 2024 untuk mengurangi serangan siber di Indonesia tidak tercapai. Perlu menjadi catatan bahwa peningkatan drastis terjadi di tahun 2022.

Skor Global Cybersecurity Index Indonesia

Sedangkan skor GCI Indonesia pada tahun 2020 menempati urutan ke-24, padahal pengguna internet di Indonesia merupakan terbanyak ke-4 di dunia. Data ini menunjukkan bahwa keamanan siber di Indonesia masih belum memadai. Berikut, merupakan data GCI pada tahun 2022:

Tabel 2 menunjukkan bahwa Indonesia menempati urutan ke-24 diantara 193 negara yang tergabung dalam ITU dan menempati urutan ke-3 di Asia Tenggara. Perlu diketahui bahwa terdapat 5 (lima) indikator dalam skor GCI, yaitu indikator *Legal, Technical, Organizational, Capacity Development,* dan *Cooperative*. Terkait skor per indikator, Indonesia mendapatkan skor 18.48 pada indikator Legal, skor 19.08 pada indikator Technical, skor 17,84 pada indikator *Organizational,* skor 19,48 pada indikator *Capacity Development*, dan skor 20,00 pada indikator Cooperative.

Tabel 2. Skor GCI Negara di Asia Tenggara Tahun 2020

Negara	Skor GCI	Ranking Dunia
Singapura	98,52	4
Malaysia	98,06	5
Indonesia	94,88	24
Vietnam	94,59	25
Thailand	86,5	44
Filipina	77	61
Brunei Darussalam	56,07	85
Myanmar	36,41	99
Laos	20,34	131
Kamboja	19,12	132
Timor Leste	4,26	173

Sumber: Global Cybersecurity Index 2020 (2021)

Melihat hal tersebut, Indonesia masih harus mengoptimalkan indikator *Organizational*. Skor per indikator mengindikasikan bahwa untuk Indonesia kinerja organisasi atau instansi terkait keamanan siber belum maksimal. Masih tingginya serangan siber dan masih relatif rendahnya indeks keamanan siber di Indonesia mengindikasikan bahwa penguatan keamanan siber di Indonesia masih belum sepenuhnya efektif. Peneliti keamanan siber, Ibnu Dwi Cahyo (2024) mengatakan bahwa beberapa hambatan besar dalam usaha penguatan keamanan siber adalah belum adanya roadmap jelas terkait keamanan siber di Indonesia, masih rendahnya kualitas Sumber Daya Manusia (SDM) terkait keamanan siber, dan awareness masyarakat Indonesia terkait keamanan siber masih rendah.

Hal ini senada dengan temuan Badan Pemeriksa Keuangan Republik Indonesia (BPK RI) dalam pemeriksaan kinerja terkait keamanan dan ketahanan siber di Kemenkominfo pada tahun 2022 yang menjelaskan bahwa terdapat kekurangan SDM keamanan siber, tidak adanya program pengembangan kompetensi SDM terkait keamanan dan ketahanan siber, dan kerja sama antar instansi terkait keamanan dan ketahanan siber yang belum mengatur output dan *outcome* secara jelas.

Selain itu, BPK RI menjelaskan bahwa di program yang meningkatkan awareness masyarakat terkait dunia digital yaitu program Literasi Digital terdapat kelemahan pada sisi perencanaan yaitu target program tidak merinci pengguna internet aktif ataupun pasif, padahal yang sangat memerlukan sosialisasi adalah pengguna internet aktif.

PENUTUP

Meningkatnya serangan siber di Indonesia, masih relatif rendahnya indeks keamanan siber Indonesia, dan beberapa temuan BPK RI menunjukkan bahwa penguatan keamanan siber di Indonesia masih belum sepenuhnya efektif. Hal ini diperparah dengan adanya tren penurunan anggaran teknis untuk program keamanan dan ketahanan siber, maka patut dipertanyakan komitmen pemerintah dalam penguatan keamanan siber. Dalam rangka penguatan Keamanan Siber di Indonesia, DPR RI melalui Komisi I perlu untuk berperan aktif dengan melakukan sebagai berikut:

1. Mendorong adanya Roadmap Keamanan Siber Nasional yang jelas dan terstruktur lengkap dengan output dan outcome.
2. Meminta penjelasan BSSN terkait tren penurunan yang terjadi di Program Keamanan dan Ketahanan Siber
3. Mendorong pemerintah untuk memiliki rencana penguatan kualitas dan kecukupan SDM keamanan siber dengan bekerja sama dengan lembaga pendidikan negeri maupun swasta.

DAFTAR PUSTAKA

Badan Pemeriksa Keuangan Republik Indonesia. (2019). Laporan Hasil Pemeriksaan atas Laporan Keuangan Badan Siber dan Sandi Negara Tahun 2018. Jakarta: BPK RI.

Badan Pemeriksa Keuangan Republik Indonesia. (2020). Laporan Hasil Pemeriksaan atas Laporan Keuangan Badan Siber dan Sandi Negara Tahun 2019. Jakarta: BPK RI.

Badan Pemeriksa Keuangan Republik Indonesia. (2021). Laporan Hasil Pemeriksaan atas Laporan Keuangan Badan Siber dan Sandi Negara Tahun 2020. Jakarta: BPK RI.

Badan Pemeriksa Keuangan Republik Indonesia. (2022). Laporan Hasil Pemeriksaan atas Laporan Keuangan Badan Siber dan Sandi Negara Tahun 2021. Jakarta: BPK RI.

Badan Pemeriksa Keuangan Republik Indonesia. (2022). Laporan Hasil Pemeriksaan atas Keamanan dan Ketahanan Siber dalam Rangka Mendukung Stabilitas Keamanan Nasional pada Kementerian Komunikasi dan Informatika dan Instansi terkait Lainnya. Jakarta: BPK RI.

Badan Siber dan Sandi Negara. (2019). Laporan Tahunan Honeynet Project BSSN – IHP 2018. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2020). Laporan Tahunan Honeynet Project BSSN – IHP 2019. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2021). Laporan Tahunan Honeynet Project BSSN – IHP 2020. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2022). Laporan Tahunan Honeynet Project BSSN – IHP 2021. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2023). Laporan Tahunan Honeynet Project BSSN – IHP 2022. Jakarta: BSSN.

Cahyo, Ibnu Dwi. (2024). Ancaman Siber Terkini. Focus Group Discussion dengan Tema “Menguji Efektivitas Pelaksanaan Program Bidang Perlindungan Sosial, Pemberdayaan Masyarakat, Pendidikan dan Keamanan Dalam APBN” dan Sub Tema “Efektifitas Penguatan Keamanan Siber Indonesia”, Bogor 16 Januari 2024.

Herdiana, Yudi, Zen Munawar, dan Novianti Indah Putri. (2021). Mitigasi Ancaman Resiko Keamanan Siber di Masa Pandemi Covid-19. Jurnal ICT: Information Communication & Technology Vol. 21, No.1, Juli 2021.

International Telecommunication Union. (2021). Global Cybersecurity Index 2020. ITU Publications.