BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital telah membawa dampak signifikan dalam berbagai sektor kehidupan, termasuk sektor pemerintahan di Indonesia. Perkembangan TIK telah memungkinkan penerapan sistem pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada masyarakat secara efisien dan transparan. Perkembangan teknologi informasi dan komunikasi (TIK), telah membawa Sistem Pemerintahan Berbasis Elektronik potensi besar untuk meningkatkan efisiensi, transparansi, dan pelayanan publik yang berkualitas. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE. Hal ini sebagaimana yang tertuang pada Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.[1] SPBE bertujuan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya.

Menurut data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023 jumlah penetrasi internet di Indonesia telah mencapai 78,19% atau menembus 215.626.156 jiwa dari total populasi yang sebesar 275.773.901 jiwa.[2] Namun seiring dengan perkembangan ini, keamanan siber juga menjadi perhatian utama. Karena semakin banyaknya data yang dipertukarkan melalui platform elektronik, risiko keamanan siber juga semakin tinggi dan kompleks. Laporan Lanskap Keamanan Siber Indonesia Tahun 2022 Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa total trafik anomali di Indonesia selama tahun 2022 mencapai 976.429.996 anomali, dengan jenis trafik anomali tertinggi adalah MyloBot Botnet, yang memungkinkan penyerang mengambil kendali penuh atas sistem pengguna.

[1] Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik
[2] https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang

Selain itu, terdapat 4.421.992 aktivitas APT dan 2.348 kasus *Web Defacement* yang terjadi di Indonesia pada tahun 2022.

Dari laporan aduan siber stakeholder yang diterima BSSN, tercatat sebanyak 236 aduan, yang didominasi oleh sektor administrasi pemerintahan dengan kategori *misconfiguration*. Selain itu, BSSN juga telah mengirimkan 1.433 notifikasi indikasi insiden kepada para stakeholder seperti *web defacement*, dugaan insiden siber yang mencapai 399 dengan dugaan kebocoran (*data breach*) paling banyak ditemukan, serta kasus peretasan web pemerintah dengan teknik *web defacement* atau penggantian tampilan website dengan halaman tertentu diantaranya terjadi 885 kasus pada tahun 2022, dan 161 kasus pada tahun 2023.[3,4] Kemudian melalui penelusuran darknet ditemukan juga akun kredensial (*credential exposure*) yang berdampak pada 427 stakeholder di Indonesia.[5]

Di sisi lain kebocoran data menjadi salah satu isu yang paling aktual saat ini, terutama ketika menargetkan kementerian dan lembaga di Indonesia. Pada tahun 2021 setidaknya terdapat kasus kebocoran data di Indonesia diantaranya meliputi: Facebook (April 2021), BPJS Kesehatan (Mei 2021), BRI Life (Juli 2021), eHAC (Agustus 2021), Sertifikat Vaksin Jokowi (September 2021), KPAI (Oktober 2021), Bank Jatim (Oktober 2021), dan Database Polri (November 2021).[6] Selanjutnya pada tahun 2022 setidaknya telah terjadi 10 insiden yang diduga kebocoran data yang menargetkan instansi seperti: Bank Indonesia (Januari 2022), Data Pasien Rumah Sakit (Januari 2022), Data Pelamar Kerja PT. Pertamina Training & Consulting (Januari 2022), Data 21.000 Perusahaan di Indonesia (Agustus 2022), Data Pelanggan PLN (Agustus 2022), Data Pengguna IndiHome (Agustus 2022), Data Pelanggan Jasa Marga (Agustus 2022), Data SIM Card Indonesia (September 2022), Data KPU (September 2022), dan Data My Pertamina (November 2022).[7]

---

[3] BSSN. Lanskap Keamanan Siber Indonesia 2022

[4] BSSN. Hasil Monitoring Keamanan Siber Direktorat Operasi Keamanan Siber, (diolah Peneliti, 2023)

[5] BSSN. Lanskap Keamanan Siber Indonesia 2022

[6] Suara.com. *Daftar Kasus Kebocoran Data di Indonesia selama 2021, Termasuk Sertifikat Vaksin Jokowi* (2023), diakses dari https://www.suara.com/tekno/2022/01/01/015822/daftar-kasus-kebocoran-data-di-indonesia-selama-2021-termasuk-sertifikat-vaksin-jokowi

[7] Teknologi.bisnis.com. *Kaleidoskop 2022: Daftar 10 Kasus Kebocoran Data di Indonesia*, diakses dari https://teknologi.bisnis.com/read/20221219/84/1609866/kaleidoskop-2022-daftar-10-kasus-kebocoran-data-di-indonesia

Kemudian kasus ini tidak berhenti di tahun 2023, Data BPJS Ketenagakerjaan (Maret 2023), Data Nasabah Bank Syariah Indonesia (Mei 2023), dan Kebocoran Data Pasport Indonesia (Juli 2023) menjadi isu terbaru dalam dugaan kasus kebocoran data ini. BSSN melalui Tim Monitoring Keamanan Siber, Direktorat Operasi Keamanan Siber juga mendeteksi adanya dugaan kebocoran data. Pada tahun 2022 setidaknya terdapat 311 notifikasi Indikasi dugaan kebocoran data, dan 193 notifikasi indikasi dugaan kebocoran data pada tahun 2023.[8]

Melihat berbagai insiden di atas, keamanan siber menjadi isu yang semakin penting bagi pemerintah dan industri bisnis, kaitannya dengan era transformasi digital. Kolaborasi antar pihak di sektor TIK menjadi sangat penting. Pemerintah berharap program keamanan siber dilakukan secara bersama-sama, jangan semua tanggung jawab diberikan kepada pemerintah. Segala upaya dalam pelaksanaan keamanan siber perlu berlandaskan pada kolaborasi yang efektif diantara seluruh pemangku kepentingan melalui penguatan peran yang meliputi pemerintah, pelaku usaha, akademisi, dan masyarakat.[9] Pada sektor administrasi pemerintahan menunjukkan bahwa aspek keamanan siber merupakan salah satu unsur penting dalam penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia. Hal ini sebagaimana amanat yang tertuang dalam:

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 16 (1) yang menyatakan bahwa

> *"Penyelenggara Sistem Elektronik harus dapat melindungi ketersediaan, keutuhan, kerahasiaan, dan keteraksesan informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut".*[10]

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 23 yang menyatakan bahwa:

> *"Penyelenggaraan sistem elektronik wajib melakukan pengamanan terhadap komponen sistem elektronik".*[11]

---

[8] BSSN. Hasil Monitoring Keamanan Siber, Direktorat Operasi Keamanan Siber, (diolah Peneliti, 2023)

[9] https://tekno.republika.co.id/berita/r4jmmm374/keamanan-siber-makin-penting-pada-era-transformasi-digital

[10] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[11] Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik Pasal 41 ayat (1), yang menyatakan bahwa:

> *"Setiap Instansi Pusat dan Pemerintah Daerah Harus Menerapkan Keamanan SPBE".*[12]

Peraturan Presiden Republik Indonesia 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik, memuat gambaran tentang:

> *"kerangka dasar yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terintegrasi."*

Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital yang memberikan amanat untuk:

> *"melindungi keberlangsungan penyelenggaraan IIV secara aman, andal, dan tepercaya; mencegah terjadinya gangguan, kerusakan, dan/ atau kehancuran pada IIV akibat serangan siber, dan/ atau ancaman/kerentanan lainnya; dan meningkatkan kesiapan dalam menghadapi Insiden Siber dan mempercepat pemulihan dari dampak Insiden Siber."*

Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber memberikan amanat tentang:

> "*Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber merupakan acuan bagi Instansi Penyelenggara Negara dan Pemangku Kepentingan untuk mewujudkan kekuatan dan kapabilitas siber dalam rangka mencapai stabilitas Keamanan Siber".*[13]

Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, Pasal 17 Ayaat (1):

> "*Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan SPBE*".

Merujuk amanat Peraturan Presiden Nomor 95 Tahun 2018 Keamanan SPBE merupakan pengendalian keamanan yang terpadu dalam SPBE, yaitu memenuhi jaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan

[12] Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

[13] Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

terhadap sumber daya yang mendukung SPBE.[14] Selain itu keamanan SPBE merupakan hal yang harus diterapkan oleh instansi pemerintah pusat dan pemerintah daerah guna mendukung penyelenggaraan SPBE yang aman dari berbagai ancaman serangan siber.[15]

BSSN melalui Direktorat Operasi Keamanan Siber menjalankan tugas dalam melakukan koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber.[16] Hal ini juga selaras dengan *Cyber Security Framework* yang diterbitkan NIST sebagai salah satu kerangka kerja keamanan teknologi informasi yang dapat digunakan dalam peningkatan keamanan infrastruktur kritis.[17] Dalam *Cyber Security Framework*, terdapat lima fungsi dalam siklus hidup keamanan (*life cycle*) siber, di antaranya seperti: identifikasi (*identify*), proteksi (*protect*), deteksi (*detect*), tanggap (*response*) dan pemulihan (*recovery*). Fungsi Identifikasi dan Proteksi, Direktorat Operasi Keamanan Siber menyediakan layanan identifikasi berupa *Information Technology Security Assessment* (ITSA), yang juga dikenal sebagai kegiatan *penetration testing* (*pentest*).

Menurut Bacudio, A. G., dkk (2011), pengujian keamanan siber memberikan manfaat penting bagi sebuah organisasi, baik dari perspektif bisnis maupun operasional. Selain itu, kegiatan ini dapat menjadi dasar bagi pimpinan dalam mengambil keputusan investasi di bidang keamanan siber. Sedangkan dari perspektif operasional, ITSA membantu menyusun strategi keamanan informasi dengan proses identifikasi kerentanan yang cepat dan akurat.[18] Namun dalam operasionalnya, stakeholder pemilik sistem elektronik sering kali terkendala dengan pelaksanaan kegiatan identifikasi kerentanan dan proteksi akibat belum terpenuhinya SDM keamanan siber yang mengawaki di organisasi tersebut.

---

[14] Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

[15] *Loc.cit*, pasal 41

[16] Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 Tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara

[17] NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity*, diakses dari https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[18] Bacudio, A. G., Yuan, X., Chu, B. B.-T., & Jones, M. (2011). *An Overview of Penetration Testing*. International Journal of Network Security & Its Applications (IJNSA), 3(6), 19. DOI: 10.5121/ijnsa.2011.3602.

Tito Rachmanto (2023) menjelaskan bahwa SDM yang memiliki kompetensi TIK merupakan salah satu pondasi yang harus terbangun di era SPBE.[19] Sejalan dengan hal tersebut, Juru Bicara (Ariandi Putra) kebutuhan SDM keamanan siber di seluruh instansi kementerian/lembaga mencapai 8.250 orang. Sedangkan kebutuhan SDM keamanan siber di sektor industri mencapai 9.804 orang. Sehingga, total kebutuhan personil SDM keamanan siber mencapai 18.054 orang. BSSN secara khusus juga membentuk SDM keamanan siber melalui Politeknik Siber dan Sandi Negara (Poltek SSN).[20]

Vulnerability Disclosure Program (VDP) dan *Bug Bounty Program* (BBP) merupakan program kolaborasi antara pemilik sistem elektronik, para pencari kerentanan dan penyelenggara program. VDP adalah program yang memberikan panduan jelas tentang bagaimana sebuah organisasi ingin diberitahu tentang potensi kerentanan keamanan yang ditemukan oleh pihak ketiga eksternal. Sedangkan BBP untuk menemukan kerentanan keamanan pada organisasi dan melaporkannya ke organisasi terkait sehingga dapat diatasi dengan aman dan organisasi akan memberikan insentif kepada pihak pelapor berupa hadiah uang.[21] A.T. Chatfield dan C.G. Reddick (2017) berpendapat bahwa mengenai pencarian dan identifikasi kerentanan pada sistem pemerintah dapat dilakukan dengan konsep Program Penghargaan Kerentanan (*Vulnerability Reward Program* - VRP). Program ini diterapkan untuk mendapatkan kerentanan keamanan siber pada Departemen Pertahanan Pentagon AS dengan melibatkan partisipasi dari Pegiat keamanan siber yang menemukan 1.189 kerentanan aplikasi, dan 138 di antaranya diterima sebagai valid dan belum diungkapkan sebelumnya. Program ini menghabiskan biaya $150.000, tetapi program ini dapat menghemat anggaran dari Departemen Pertahanan lebih dari $1 juta dibandingkan dengan menggunakan konsep audit keamanan secara tradisional.[22] Walshe, T., & Simpson, A.C (2022) menunjukkan

---

[19] Rachmanto, Tito (2023) *Analisis Kompetensi Sumber Daya Manusia Teknologi Informasi dan Komunikasi Dinas Komunikasi dan Informatika Pemerintah Kota Surabaya dalam Sistem Pemerintahan Berbasis Elektronik.* Masters Thesis, Universitas 17 Agustus 1945 Surabaya, diakses dari http://repository.untag-sby.ac.id/26118/

[20] https://www.medcom.id/nasional/politik/8Kyzja2N-bssn-dibutuhkan-18-ribu-personel-sdm-untuk-keamanan-siber, diakses pada 2 November 2023

[21] https://docs.hackerone.com/organizations/vdp-vs-bbp.html

[22] A.T. Chatfield, and C.G. Reddick. 2017. DIO Proceedings Paper. In *Proceedings of DGO conference, Staten Island, NY USA, June 2017*, pages 10

bahwa Program *Bug Bounty* dan Program Pengungkapan Kerentanan dapat menjadi jenis program yang efektif, dan mempengaruhi perubahan dalam pengembangan aplikasi melalui konsep *Software Development Life Cycle* (SDLC) dalam pengembangan aplikasi akan menerapkan kaidah-kaidah yang lebih aman.[23] Sejalan dengan hal tersebut Monash University, Australia juga menjalankan Program Pengungkapan Kerentanan untuk meminimalkan dampak potensial kerentanan keamanan, melindungi kerahasiaan, integritas, dan ketersediaan informasi dan platform digitalnya.[24] Selain itu terdapat praktik serupa di negera-negara lain seperti Singapura, Belanda, India, Arab Saudi, dan Indonesia.

Di Indonesia sudah muncul beberapa program pencarian kerentanan pada suatu sistem elektronik, sebagai contoh program *bug bounty* yang diselenggarakan oleh CyberArmyID, yaitu entitas layanan keamanan siber berbasis kerumunan yang memungkinkan individu untuk berpartisipasi dalam penyelesaian masalah keamanan siber dengan cara yang aman dan terkontrol.[25] Gojek juga memiliki program *bug bounty* yang dibuka secara umum bagi peretas dan peneliti keamanan siber yang bekerja sama dengan HackerOne. Untuk dapat ikut serta, peretas dan peneliti etis dapat terlebih dahulu melakukan pengujian serta analisis individual yang dapat dikirimkan melalui platform HackerOne.[26] Begitupun sektor *e-commerce*, Tokopedia juga menyelenggarakan *Program Bug Bounty* dengan memberikan apresiasi berupa uang pada setiap kerentanan yang diterima dan valid.[27] Sedangkan dari sektor pemerintah telah menyelenggarakan program pencarian kerentanan terhadap sistem elektronik pada lingkup-lingkup organisasinya, diantaranya seperti: Dinas Komunikasi dan Informatika Provinsi Jawa Barat membuat semacam program pemburuan celah keamanan,tapi bukan *bug bounty* Tahun 2019, Pemerintah Kabupaten Serang Tahun 2020, Pemerintah

[23] Walshe, T., & Simpson, A.C. (2022). *Coordinated Vulnerability Disclosure Programme Effectiveness: Issues and Recommendations. Computers & Security*, 123, 102936. https://doi.org/10.1016/j.cose.2022.102936

[24] https://www.monash.edu/report-security-vulnerabilities, diakses pada 4 November 2023

[25] https://app.cyberarmy.id/bug-bounty-program, diakses pada 2 November 2023

[26] https://hackerone.com/gojek?type=team, diakses pada 2 November 2023

[27] https://bounty.tokopedia.net/rules, diakses pada 4 November 2023

Provinsi Bali melalui Bali Digifest 2023, Kemendikbud melalui program *Bug Bounty Competition* 2023.[28,29,30,31]

Sejak Tahun 2019 BSSN telah merilis program *Voluntary Vulnerability Disclosure Program* (VVDP). Program ini merupakan program yang mengakomodir para pegiat keamanan siber untuk membantu para pemilik sistem dalam mengidentifikasi kerentanan sistemnya secara sukarela. Namun program tersebut sempat dihentikan akibat terbatasnya Sumber Daya Manusia dan Anggaran yang memadai, serta belum ada aturan yang kuat untuk menyelenggarakan program.[32] Namun antusiasme pada pencari kerentanan (*bug hunter*) ini tidak padam dan surut, dalam periode tahun 2020 – 2023 sudah masuk sejumlah 1.604 laporan yang masuk ke BSSN terkait temuan kerentanan dari sistem elektronik milik pemerintah.[33]

Tingginya jumlah laporan yang diterima menunjukkan banyaknya kerentanan pada sistem milik pemerintahan. Di sisi lain, hal itu juga menunjukkan besarnya potensi yang dimiliki komunitas *bug hunter* di Indonesia. Namun dalam pelaksanaannya juga tidak lepas dari permasalahan, seperti permasalahan apresiasi yang akan diberikan kepada partisipan seperti pelapor, perjanjian kerjasama, mekanisme validasi dan verifikasi peserta, sistem elektronik, verifikasi laporan, pemberian apresiasi, dan mekanisme pemberian sanksi.[34]

Dalam rangka pelaksanaan fungsi tersebut dan untuk memperluas cakupan layanan Identifikasi dan Proteksi, serta dalam rangka membuka partisipasi masyarakat dalam meningkatkan iklim keamanan siber di Indonesia, maka BSSN membentuk program Identifikasi Kerentanan dan Proteksi Secara Sukarela BSSN. Program ini diharapkan menjadi wadah dalam menciptakan kolaborasi yang baik

---

[28] https://cyberthreat.id/read/4347/Pemprov-Jabar-Akan-Adakan-Kegiatan-Sejenis-Bug-Bounty, diakses pada 2 November 2023

[29] https://inilahbanten.co.id/detail/bug-bounty-program-pemkab-serang-apresiasi-bug-hunter/, diakses pada 2 November 2023

[30] https://digifest.baliprov.go.id/?lang=en, diakses pada 2 November 2023

[31] https://www.kemdikbud.go.id/main/blog/2023/08/ajang-bug-bounty-competition-2023-tarik-minat-mahasiswa, diakses pada 2 November 2023

[32] https://www.cyberthreat.id/read/7183/BSSN-Hentikan-Sementara-Program-untuk-White-Hacker, diakses pada 2 November 2023

[33] BSSN. Data Rekapitulasi Laporan Kerentanan dari Bug Hunter (diolah Peneliti, 2023)

[34] https://twitter.com/secgron/status/1434369316472770562, diakses pada 2 November 2023

antara Pemerintah dengan Pegiat keamanan siber di Indonesia, untuk bersama-sama menjaga keamanan siber di Indonesia khususnya dalam identifikasi kerentanan, dan bagaimana memberikan rekomendasi pengamanan pada sistem elektronik milik suatu organisasi. Pengaturan penyelenggaraan program ini terdiri atas: penyelenggara program identifikasi kerentanan dan proteksi secara sukarela; peserta program identifikasi kerentanan dan proteksi secara sukarela; pendaftaran dan verifikasi; pelaksanaan program identifikasi kerentanan; pelaksanaan program proteksi; pemantauan dan evaluasi; publikasi kerentanan; pemberian apresiasi dan sanksi; dan penyimpanan dan pengelolaan informasi. Pihak-pihak yang terlibat pada Program Identifikasi Kerentanann dan Proteksi secara Sukarela BSSN terdiri atas BSSN sendiri selalu penyelenggara program, pengidentifikasi, pemberi rekomendasi keamanan dan penyeleggara sistem elektronik lingkup publik (pemilik sistem).[35]

Untuk menyongsong pelaksanaan program Identifikasi Kerentanan dan Proteksi Secara Sukarela, BSSN telah menyelenggarakan beberapa kegiatan diantaranya webinar, konsolidasi dengan PSE Lingkup Publik dan para pegiat keamanan siber, serta Pilot Project Penyelenggaraan Program Identifikasi Kerentanan dan Proteksi secara Sukarela dengan berkolaborasi bersama stakeholder terkait. Beberapa kegiatan pilot project maupun kolaborasi kegiatan persiapan diantaranya diselenggarakan bersama Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi, Kementerian Keuangan, dan Pemerintah Provinsi Bali, Pemerintah Pronvinsi Jawa Tengah, dan Pemerintah Pronvinsi Jawa Timur. Dari kegiatan tersebut telah memberikan gambaran bagaimana mekanisme penyelenggaraan program identifikasi kerentanan dan proteksi secara sukarela. [36]

Melalui pelaksanaan program Identifikasi Kerentanan dan Proteksi secara Sukarela diharapkan dapat memberikan manfaat yang merata di seluruh pihak yang terlibat. Pemerintah Indonesia dapat meningkatkan keamanan siber nasional dengan melibatkan masyarakat dan pegiat keamanan siber dalam mengidentifikasi potensi kerentanan dalam sistem elektronik di lingkup publik. Kolaborasi yang

[35] Peraturan Kepala Badan Siber dan Sandi Negara Nomor 5 Tahun 2023 tentang Penyelenggaraan Program Identifikasi Kerentanan dan Proteksi Secara Sukarela

[36] BSSN. Hasil Kolaborasi Program Identifikasi Kerentanan dan Proteksi secara Sukarela, Direktorat Operasi Keamanan Siber (diolah Peneliti, 2024)

terjalin dapat mempercepat deteksi kerentanan dan penanganan masalah keamanan siber. Pegiat keamanan siber dan masyarakat mendapatkan kesempatan untuk aktif berpartisipasi dalam upaya meningkatkan keamanan siber, dengan memberikan rekomendasi keamanan dan memperkaya pengetahuan mereka. Pemilik sistem elektronik, seperti instansi pemerintah pusat dan daerah mendapatkan manfaat dalam bentuk rekomendasi keamanan yang dapat membantu melindungi sistem mereka dari potensi ancaman. Selain itu, BSSN sebagai penyelenggara program dapat memperoleh informasi terkini tentang kerentanan dan proteksi sistem elektronik di Indonesia, membangun kolaborasi lintas sektor, dan memfasilitasi upaya bersama untuk meningkatkan keamanan siber nasional.

Seluruh masyarakat juga dapat menikmati manfaat dari program ini dengan adanya peningkatan keamanan siber secara keseluruhan. Melalui partisipasi aktif dalam identifikasi kerentanan dan proteksi, setiap individu dapat menjadi bagian dari upaya kolektif untuk melindungi informasi dan data sensitif. Kesadaran akan keamanan siber pun dapat meningkat di kalangan masyarakat, mengingat pentingnya peran setiap pihak dalam menjaga keamanan informasi dalam era digital. Dengan demikian, program ini tidak hanya memberikan manfaat langsung kepada pihak yang terlibat secara langsung, tetapi juga menciptakan dampak positif yang lebih luas dalam memperkuat ketahanan keamanan siber di Indonesia.

Menurut Suryono (2001), sebagaimana dikutip oleh Mary Ismowati, dkk (2022), partisipasi masyarakat dalam pembangunan diartikan sebagai ikut sertanya masyarakat dalam pembangunan, ikut dalam kegiatan pembangunan, dan ikut serta memanfaatkan serta menikmati hasil-hasil pembangunan. Mary Ismowati, dkk (2022) menjelaskankan bahwa rendahnya partisipasi masyarakat di penelitiannya, akibat kurangnya pemberdayaan, pelatihan, edukasi, dan pemahaman masyarakat tentang bidang yang dikelolanya. Oleh karena itu, diperlukan upaya yang lebih baik dalam meningkatkan partisipasi masyarakat.[37]

[37] Mary Ismowati, Bhakti Nur Avianto, Angga Sulaiman, Anggra Liany Rihadatul Aisi, & Vicky Zaynul Firmansyah, "Edukasi Pariwisata dan Aksi Sisir Pantai dari Sampah Wisata dalam Upaya Meningkatkan Partisipasi Masyarakat di Kawasan Super Prioritas Nasional (KSPN) Labuan Bajo, Kabupaten Manggarai Barat," *Jurnal Komunitas: Jurnal Pengabdian kepada Masyarakat* 5, no. 1 (Juli 2022): 12-21, DOI: https://doi.org/10.31334/jks.v5i1.2288

Selaras dengan hal tersebut, peningkatan keamanan aplikasi SPBE melalui kolaborasi tidak akan berjalan sukses tanpa adanya mekanisme yang jelas, dan objektif yang jelas. Apresiasi pada program VVDP BSSN menjadi salah satu faktor yang perlu didalami dan diperjelas. Hal ini ditujukan untuk menghindari persepsi dari para pelapor terhadap keseriusan pemerintah dalam menyelenggarakan program partisipasi masyarakat terhadap keamanan siber di Indonesia. Teguh Aprianto sebagai salah satu pegiat keamanan siber juga telah menyampaikan agar BSSN selaku penyelenggara dapat memberikan aspirasi yang lebih bernilai.[38]

Kolaborasi tidak akan tercapai apabila tidak ada sesuatu yang didapatkan di masing-masing pihak yang terlibat dalam kerja sama tersebut, baik itu apresiasi maupun imbalan senilai dengan pekerjaan yang dilakukan. Menurut Nawawi dalam Pratama,dkk (2015), imbalan adalah usaha menumbuhkan perasaan diterima (diakui) di lingkungan kerja, yang menyentuh aspek kompensasi dan aspek hubungan antara para pekerja yang satu dengan yang lainnya.[39] Victor Vroom menjelaskan bahwa teori imbalan didasarkan pada tiga konsep penting, yaitu harapan (*Expectancy*), nilai (*Valence*), dan instrumentalitas (*Instrumentality*). Seseorang akan termotivasi untuk melakukan suatu tindakan jika ia percaya bahwa tindakan tersebut akan menghasilkan hasil yang diinginkannya, dan hasil tersebut bernilai bagi dirinya.[40]

Dengan adanya konsep baru identifikasi kerentanan dan proteksi secara sukarela yang tidak hanya memperbaiki mekanisme pemberian aspirasi, namun mulai dari pendaftaran peserta, pendaftaran sistem elektronik yang akan diuji, mekanisme pelaporan, verifikasi laporan dan pemberian nilai, ketentuan-ketentuan terhadap yang boleh dan dilarang akan diatur lebih jelas. Sehingga ruang lingkup pengujian akan lebih fokus dan tidak terlalu luas. Dengan demikian, diharapkan pelaksanaan program VVDP yang berevolusi menjadi Program Identifikasi Kerentanan dan Proteksi secara Sukarela BSSN akan lebih baik.

---

[38] https://x.com/secgron/status/1434369316472770562?s=20, diakses pada 2 November 2023

[39] Kwik Kian Gie. BAB II KAJIAN PUSTAKA A. 1. a. Pengertian Imbalan, diakses dari http://eprints.kwikkiangie.ac.id/894/3/BAB%20II%20KAJIAN%20PUSTAKA.pdf.

[40] Unsri. BAB II TINJAUAN PUSTAKA 2.1 Landasan Teori 2.1.1. Teori harapan Victor Vroom. https://repository.unsri.ac.id/765/2/RAMA_62201_01031381419159_0010126703_0001076702_02.%20pdf.pdf.

Selanjutnya dari sisi penyelenggara, BSSN juga perlu memperhatikan personil yang terlibat dalam tim penyelenggara. I Made Adnyana dan Asadini Dwi Ajeng Gemellia (2019) menjelaskan bahwa fleksibilitas kerja, keseimbangan kehidupan kerja, penghargaan dan lingkungan kerja non fisik masing-masing berpengaruh positif dan signifikan terhadap kinerja pegawai BSSN. Sementara sebuah penghargaan memberikan pengaruh terkuat dan lingkungan kerja non fisik juga memberikan pengaruh terhadap kinerja pegawai BSSN, meskipun tidak signifikan.[41]

Melalui penelitian ini, diharapkan kolaborasi antara Pemerintah dan Masyarakat dalam Program Identifikasi Kerentanan dan Proteksi Secara Sukarela BSSN dapat menjadi langkah strategis dalam meningkatkan keamanan siber SPBE di Indonesia. Penelitian ini akan menganalisis secara mendalam proses bisnis penyelenggaraan program tersebut dengan menggunakan model *Collaborative Governance* Tonelli, Sant'anna, Abbud, dan De Souze (2018), yang membagi proses kolaborasi menjadi tiga dimensi utama: *Antecedents*, *Collaborative Process*, dan *Equity Outcomes*. Analisis ini akan mencakup persiapan kolaborasi, pelaksanaan kolaborasi, dan hasil yang adil dari masing-masing pihak yang terlibat. Dengan pendekatan ini, diharapkan penelitian dapat memberikan pemahaman yang lebih mendalam terhadap konsep kolaborasi yang diusung oleh BSSN dalam Program Identifikasi Kerentanan dan Proteksi Secara Sukarela, sehingga dapat dijadikan sebagai alternatif bagi pemerintah dalam upaya peningkatan keamanan Sistem Pemerintahan Berbasis Elektronik di Indonesia, khususnya melalui proses identifikasi kerentanan dan proteksi.

1.2 Rumusan Masalah dan Pertanyaan Penelitian

Dari ulasan latar belakang yang telah dituliskan, terdapat beberapa masalah yang mempengaruhi penyelenggaraan SPBE, seperti masih tinggi insiden siber yang menargetkan sistem pemerintah, masih tingginya permintaan layanan identifikasi dan pengujian keamanan aplikasi ke BSSN, aktivitas pegiat keamanan siber lokal yang sangat aktif ingin membantu pemerintah dalam hal keamanan siber,

[41] I Made Adnyana and Asadini Dwi Ajeng Gemellia, "Analisis Kinerja Aparatur Sipil Negara di Badan Siber dan Sandi Negara Tahun 2019," *Populis: Jurnal Sosial dan Humaniora* 6, no. 2 (2021): 211, http://journal.unas.ac.id/populis/article/view/1387/1054

adanya konsep Identifikasi Kerentanandan Proteksi secara Sukarela, Kolaborasi BSSN dengan pegiat keamanan siber belum maksimal, dan pemberian apresiasi masih menjadi salah satu kendala utama dalam penyelenggaran Identifikasi Kerentanandan Proteksi secara Sukarela. Berikut merupakan rumusan masalah penelitian yang difokuskan pada tiga hal, yaitu:

1. Bagaimana kolaborasi pemerintah dan masyarakat dalam Program Identifikasi Kerentanan dan Proteksi Secara Sukarela Badan Siber dan Sandi Negara sebagai upaya peningkatan keamanan Sistem Pemerintahan Berbasis Elektronik?
2. Faktor apa yang mendukung dan menghambat proses kolaborasi pemerintah dan masyarakat dalam Program Identifikasi Kerentanan dan Proteksi Secara Sukarela Badan Siber dan Sandi Negara?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisis kolaborasi pemerintah dan masyarakat dalam Program Identifikasi Kerentanan dan Proteksi Secara Sukarela Badan Siber dan Sandi Negara sebagai upaya peningkatan keamanan Sistem Pemerintahan Berbasis Elektronik; dan untuk mengetahui faktor-faktor yang mendukung dan menghambat proses kolaborasi pemerintah dan masyarakat dalam Program Identifikasi Kerentanan dan Proteksi Secara Sukarela Badan Siber dan Sandi Negara.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritias maupun secara praktis, yaitu:

1. Secara teoritis, diharapkan penelitian ini dapat menambah dan memperluas pengetahuan yang berkaitan dengan kolaborasi pemerintah dan masyarakat dalam Program Identifikasi Kerentanan dan Proteksi Secara Sukarela Badan Siber dan Sandi Negara sebagai upaya peningkatan keamanan Sistem Pemerintahan Berbasis Elektronik.

2. Penelitian ini dapat menjadi referensi bagi peneliti-peneliti lain, dan juga dapat meningkatkan kualitas belajar, referensi berpikir, serta memberikan dan menambah ilmu pengetahuan bagi peneliti dan mahasiswa lainnya.
3. Secara praktis, penelitian ini diharapkan memberikan kontribusi dan bahan pertimbangan pentuan kebijakan bagi Direktorat Operasi Keamanan Siber BSSN, sebagai sumber bacaan bagi masyarakat umum, serta sebagai salah satu syarat dalam memperoleh gelar Magister Ilmu Administrasi Publik.

1.5 Ruang Lingkup Batasan Masalah Penelitian

Pembatasan pada ruang lingkup penelitian ditetapkan agar penelitian dapat fokus pada pokok permasalahan yang ada, dan penelitian tidak menyimpang dari sasaran yang diharapkan. Berikut merupakan ruang lingkup batasan masalah pada penelitian ini, antara lain:

1. Penelitian dilakukan terhadap strategi kolaborasi antara pemerintah, masyarakat, dan Penyelenggara Sistem Elektronik Lingkup Publik dalam Program Identifikasi Kerentanan dan Proteksi Secara Sukarela Badan Siber dan Sandi Negara sebagai upaya peningkatan keamanan Sistem Pemerintahan Berbasis Elektronik.
2. Kolaborasi dilakukan antara pemerintah dengan masyarakat, dimana pemerintah terbagi menajdi 2 (dua) pihak, yaitu BSSN selaku penyelenggara Program Identifikasi Kerentanandan Proteksi secara Sukarela, dan Penyelenggara Sistem Elektronik Lingkup Publik sebagai pemelik sistem. Adapun masyarakat bertindak sebagai peserta pengidentifikasi kerentanan dan pemberi rekomendasi keamanan aplikasi SPBE.
3. Lokus penelitian dilakukan pada Direktorat Operasi Keamanan Siber, Badan Siber dan Sandi Negara.
4. Hasil kolaborasi pengamanan berfokus pada peningkatakan keamanan aplikasi SPBE pada aplikasi yang pernah lakukan pengujian keamanan (*IT Security Assessment*) dan layanan asistensi perbaikan atau proteksi sistem elektronik oleh Direktorat Operasi Keamanan siber, BSSN.

5. Informan dalam penelitian ini merupakan pejabat BSSN pada Direktorat Operasi Keamanan BSSN, serta informan pendukung lainnya terkait topik penelitian.

1.6 Sistematika Penulisan

Sistimatika penulisan ini bertujuan untuk menggambarkan alur pemikiran penulis dari awal hingga kesimpulan akhir dengan sistematika sebagai berikut:

1. BAB I PENDAHULUAN

   Bab ini didalamnya menjelaskan mengenai Latar Belakang, Identifikasi Masalah, Rumusan Masalah dan Pertanyaan Penelitian, Tujuan dan Manfaat Penelitian, Ruang Lingkup Batasan Masalah, dan Sistimatika Penulisan.
2. BAB II TINJAUAN PUSTAKA

   Bab ini didalamnya menjelaskan mengenai dasar penulisan terkait Tinjauan Studi Empiris yang menggambarkan penelitian terdahulu, Tinjauan Teoritis tentang *Collaborative Governance*, Sistem Pemerintah Berbasis Elektronik, Keamanan Siber, Keamanan SPBE, Program Pengungkapan Kerentanan Secara Sukarela, Program Identifikasi Kerentanann dan Proteksi secara Sukarela, dan konsep pendukung lainnya serta penjelasan tentang Kerangka Pemikiran Penelitian.
3. BAB III METODOLOGI PENELITIAN

   Bab ini didalamnya menjelaskan mengenai Jenis Penelitian, Jenis dan Sumber Data, Informan Penelitian, Metode Pengumpulan Data, Metode Analisis Data, dan Waktu dan Tempat Penelitian.
4. BAB IV PEMBAHASAN

   Bab ini didalamnya menjelaskan mengenai Deskripsi Data Penelitian mulai dari Deskripsi Tempat Penelitian, analisis hasil penelitian, dan pembahasan hasil penelitian.
5. BAB V PENUTUP

   Bab ini didalamnya berisi Kesimpulan, Implikasi Penelitian dan Saran tidak lanjut dari hasil penelitian.