DAFTAR PUSTAKA

Penelitian, Jurnal:

Adnyana, I. M., & Gemellia, A. D. A. (2021). Analisis Kinerja Aparatur Sipil Negara di Badan Siber dan Sandi Negara Tahun 2019. Populis: Jurnal Sosial dan Humaniora, Volume 6, Nomor 2. pISSN: 2460-4208, eISSN: 2549-7685. Program Studi Manajemen, Universitas Nasional. http://journal.unas.ac.id/index.php/populis/article/view/1387/1054

Andani, R., Ali, Y., & Wenas, F. F. (2020). Perencanaan Sumber Daya Manusia Badan Siber dan Sandi Negara Dalam Mengatasi Ancaman Siber Untuk Mendukung Pertahanan Negara. Universitas Pertahanan RI.

Ansell, C., & Gash, A. (2008). Collaborative Governance in Theory and Practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571. https://doi.org/10.1093/jopart/mum032

Akgul, O., Grossklags, et al. (2020). The Hackers' Viewpoint: Exploring Challenges and Benefits of Bug-Bounty Programs. The 6th Workshop on Security Information Workers. Diakses dari https://www2.cs.uh.edu/~gnawali/papers/bugbounty-wsiw20.pdf

Arafah, Y., Winarso, H. (2020). Peningkatan dan Penguatan Partisipasi Masyarakat dalam Konteks Smart City. *Tataloka, 22*(1), 28-31.

Arrozaaq, D. L. C. (2016). Collaborative Governance: Studi Tentang Kolaborasi Antar Stakeholders Dalam Pengembangan Kawasan Minapolitan di Kabupaten Sidoarjo. Universitas Airlangga. Tersedia di: https://repository.unair.ac.id/67685/3/Sec.pdf

A.T. Chatfield, and C.G. Reddick. 2017. Cybersecurity Innovation in Government: A Case Study of U.S. Pentagon's Vulnerability Reward Program. DIO Proceedings Paper. In Proceedings of DGO conference, Staten Island, NY USA, June 2017, h.10.

Bugin, Burhan. (2007). *Penelitian Kualitatif*. Jakarta: Kencana Prenada Media Group.

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.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage Publications.

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. *Jurnal Dinamika Global, 7*(2), Desember 2022. ISSN: 2548-9216, E-ISSN: 2684-9399. DOI: https://doi.org/10.36859/jdg.v7i02.1187.

Handayani, M. P. (2022). Analisis Kinerja Pegawai Berbasis Faktor Struktur Organisasi, Kompetensi dan Motivasi Kerja pada Badan Siber Dan Sandi Negara Tahun 2021. Tesis magister, Universitas Nasional, Sekolah Pascasarjana Program Magister Ilmu Administrasi.

Ibrahim, A., Arief, A., & Abdullah, S. D. (2020). Keamanan Untuk Penerapan Layanan Publik Pada Sistem Pemerintahan Berbasis Elektronik (SPBE): Sebuah Kajian Pustaka Sistematis. *IJIS-Indonesian Journal on Information System, 5*(2), September. e-ISSN 2548-6438, p-ISSN 2614-7173.

Ismowati, M., Avianto, B. N., Sulaiman, A., Aisi, A. L. R., & Firmansyah, V. Z. (2022). "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*, Vol. 5, No. 1, Juli, pp. 12-21. E ISSN 2021-6434. DOI: https://doi.org/10.31334/jks.v5i1.2288

Mahsun, Mohamad. (2006). *Pengukuran Kinerja Sektor Publik*. Yogyakarta: BPFE.

Maxwell, J. A. (2013). *Qualitative Research Design: An Interactive Approach*. Sage Publications.

Midgley, J. 1986. Introduction: Social Development in Midgley J. Et All Community participation social development and the state. London: Meuthen.Co.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. Sage Publications.

Mujanah, Siti. (2019). *Manajemen Kompensasi*. Surabaya: CV. Putra Media Nusantara (PMN). ISBN : 978-602-1187-66-1.

Murdiyanto, Eko. (2020). *Metode Penelitian Kualitatif: Teori dan Aplikasi disertai contoh proposal*. Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LP2M): Universitas Pembangunan Nasiona "Veteran" Yogyakarta, 2020, h.133.

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/.

Saputra, S. R. Y. (2020). Pengaruh Penggunaan Standar Pelayanan Sertifikasi Elektronik dan Kinerja Pegawai Terhadap Kepuasan Pengguna Layanan Sertifikasi Elektronik Di Unit Pelaksana Teknis Balai Sertifikasi Elektronik Badan Siber Dan Sandi Negara. Tesis magister, Universitas Nasional, Sekolah Pascasarjana Program Magister Ilmu Administrasi.

Sugiyono. (2013). *Metode Penelitian Kuantitatif, Kualitatif DAN R & D*. Bandung: Alfabeta.

Saleh, Choirul. *Modul 01: Konsep, Pengertian, dan Tujuan Kolaborasi*. Universitas Terbuka: DAPU6107 – Edisi 1, hal 1.5 – 1.6.

Suyono. (2014). "Analisis Faktor-Faktor Yang Mempengaruhi Pemilihan Karir Sebagai Akuntan Publik (Studi Empiris Pada Mahasiswa Akuntansi Unsiq)". *Jurnal Penelitian dan Pengabdian Kepada Masyarakat UNSIQ, 1*(2), pp. 69-83. doi: https://doi.org/10.32699/ppkm.v1i2.235.

Yuswanto, A., & Wibowo, B. (2020). *Pembangunan Pusat Pengendalian Operasional Keamanan Informasi (PUSDALOPS KAMI) Guna Meningkatkan Pelayanan E-Gov dari Ancaman Kejahatan Siber*. ISSN: 2089 – 5615, E-ISSN: 2722 – 7162, diakses dari https://publikasi.mercubuana.ac.id/index.php/format/article/view/10637.

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.

Dokumen:

ISO/IEC 29147:2018 Information Technology Security Techniques Vulnerability Disclosure

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

BSSN. 2022. Lanskap Keamanan Siber Indonesia 2022. Direktorat Operasi Keamanan Siber. BSSN: Jakarta Selatan

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

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

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.

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.

Peraturan Terkait

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

Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Perpres Nomor 132 Tentang Arsitektur Sistem Pemerintahan BerBasis Eletronik.

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

Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.

Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 Tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman MKI SPBE dan STP Keamanan SPBE.

Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 Tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.

Peraturan Kepala Badan Siber dan Sandi Negara Nomor 5 Tahun 2023 Tentang Penyelenggaraan Program Identifikasi Kerentanan dan Proteksi Secara Sukarela.

Website:

Asosiasi Penyelenggara Jasa Internet Indonesia. (2023, September 20). Survei APJII: Pengguna Internet di Indonesia Tembus 215 Juta Orang. Diakses pada 2023-10-02, dari https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang

Bali Digifest, Bali Digifest, https://digifest.baliprov.go.id/?lang=en, diakses pada 2 November 2023.

Bisnis.com, Kaleidoskop 2022: Daftar 10 Kasus Kebocoran Data di Indonesia, https://teknologi.bisnis.com/read/20221219/84/1609866/kaleidoskop-2022-daftar-10-kasus-kebocoran-data-di-indonesia, diakses pada 2 November 2023.

BSSN, Pengantar Strategi Keamanan Siber Indonesia, https://bssn.go.id/strategi-keamanan-siber-nasional/, diakses pada 2 November 2023.

Bugcrowd, Vulnerability Rating Taxonomy, https://bugcrowd.com/vulnerability-rating-taxonomy, diakses pada 3 November 2023.

Cyber Army Indonesia, Bug Bounty Program, https://app.cyberarmy.id/bug-bounty-program, diakses pada 2 November 2023.

Cyber Threat ID, Pemprov Jabar Akan Adakan Kegiatan Sejenis Bug Bounty, https://cyberthreat.id/read/4347/Pemprov-Jabar-Akan-Adakan-Kegiatan-Sejenis-Bug-Bounty, diakses pada 2 November 2023.

Cyber Threat ID, BSSN Hentikan Sementara Program untuk White Hacker, https://www.cyberthreat.id/read/7183/BSSN-Hentikan-Sementara-Program-untuk-White-Hacker, diakses pada 2 November 2023.

HackerOne, Gojek Bug Bounty Program, https://hackerone.com/gojek?type=team, diakses pada 2 November 2023.

HackerOne, Vulnerability Disclosure Program (VDP) vs. Bug Bounty Program (BBP), https://docs.hackerone.com/organizations/vdp-vs-bbp.html, diakses pada 4 November 2023.

Inilah Banten, Bug Bounty Program Pemkab Serang Apresiasi Bug Hunter, https://inilahbanten.co.id/detail/bug-bounty-program-pemkab-serang-apresiasi-bug-hunter/, diakses pada 2 November 2023.

Kajian Pustaka, Reward atau Penghargaan: Pengertian, Tujuan, dan Syarat, https://www.kajianpustaka.com/2020/04/reward-atau-penghargaan-pengertian-tujuan-dan-syarat.html, diakses pada 4 November 2023.

Kamus Besar Bahasa Indonesia, Keputusan, https://kbbi.kemdikbud.go.id/entri/keputusan, diakses pada 3 November 2023.

Kamsib ID, Daftar Komunitas Cyber Security di Indonesia, https://kamsib.id/cybersec/daftar-komunitas-cyber-security-di-indonesia/, diakses pada 8 Januari 2024.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, Sistem Pemerintahan Berbasis Elektronik (SPBE), https://www.menpan.go.id/site/kelembagaan/sistem-pemerintahan-berbasis-elektronik-spbe-2, diakses pada 2 November 2023.

Kementerian Pendidikan dan Kebudayaan, Ajang Bug Bounty Competition 2023 Tarik Minat Mahasiswa, https://www.kemdikbud.go.id/main/blog/2023/08/ajang-bug-bounty-competition-2023-tarik-minat-mahasiswa, diakses pada 2 November 2023.

Medcom.id, BSSN Dibutuhkan 18 Ribu Personel SDM untuk Keamanan Siber, https://www.medcom.id/nasional/politik/8Kyzja2N-bssn-dibutuhkan-18-ribu-personel-sdm-untuk-keamanan-siber, diakses pada 2 November 2023.

Monash University, *Report Security Vulnerabilities*, https://www.monash.edu/report-security-vulnerabilities, diakses pada 4 November 2023.

Republika.co.id, Keamanan Siber Makin Penting pada Era Transformasi Digital, https://tekno.republika.co.id/berita/r4jmmm374/keamanan-siber-makin-penting-pada-era-transformasi-digital, diakses pada 2 November 2023.

Suara.com, Daftar Kasus Kebocoran Data di Indonesia Selama 2021 Termasuk Sertifikat Vaksin Jokowi, https://www.suara.com/tekno/2022/01/01/015822/daftar-kasus-kebocoran-data-di-indonesia-selama-2021-termasuk-sertifikat-vaksin-jokowi, diakses pada 2 November 2023.

Tokopedia, Tokopedia Bug Bounty Program Rules, https://bounty.tokopedia.net/rules, diakses pada 4 November 2023.

Twitter, SecGron Twitter Post, https://twitter.com/secgron/status/1434369316472770562, diakses pada 2 November 2023.

X, SecGron Twitter Post, https://x.com/secgron/status/1434369316472770562?s=20, diakses pada 2 November 2023.

Venngage, Cyber Security Framework Mind Map, https://venngage.com/templates/mind-maps/cyber-security-framework-mind-map-4f764669-28f5-411c-aa0b-6119d2c2acce.

Lampiran 1
Pedoman Wawancara

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 TAHUN 2023

Tujuan Wawancara:

Wawancara dilakukan untuk mengetahui 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 (SPBE). Selain itu untuk mengetahui kolaborasi pemerintah dan masyarakat dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela, peneliti juga ingin mendapatkan informasi mengenai faktor-faktor yang mempengaruhi dalam proses kolobaorasi tersebut. Dengan demikian diharapkan dapat tergambarkan mekanisme dan faktor yang mendukung maupun menghambat dalam kolaborasi pemerintah dan masyarakat melalui program Identifikasi Kerentanan dan Proteksi Secara Sukarela yang ditetapkan oleh BSSN.

Informan Penelitian:

Informan terbagi menjadi pegawai dengan jabatan struktural dan pegawai fungsional atau jabatan non struktural di lingkungan Direktorat Operasi Keamanan Siber, BSSN, PSE Lingkup Publik dan Pegiat keamanan siber selaku perwakilan dari masyarakat.

Kisi – Kisi Pedoman Wawancara:

Dimensi	Sub Dimensi	Indikator
Antecendents	*Multiple Actors*	Keterlibatan banyak aktor akan memberikan informasi dan sumber daya yang heterogen
	Common goals	Terdapat kesadaran, dan tujuan yang sama dalam melaksanakan kolaborasi
	Facilitative leadership	Adanya salah satu pihak yang bertindak sebagai leader untuk menginisiasi program
	Preliminary rules	Adanya aturan yang dijadikan acuan dalam penyelenggaraan program sesuai dengan perannya masing-masing
	Interdependece perception	Program hanya dapat terselenggara apanila pihak penyelenggara, pemilik sistem, dan masyarakat selaku pengidentifikasi kerentanan dan/atau pemberi rekomendasi telah tersedia dan sepakat untuk menjalankan program ini
	Initial invesment	Adanya investasi awal dari penyelenggara untuk memulai proses kolaboratif, seperti dasar hukum, tata kelola, petunjuk teknis, aturan, sumber daya keuangan, manusia, teknologi, dan dukungan lainnya, serta aset *intangible* seperti pengetahuan, status, identitas, ideologi, budaya, dan keterampilan yang mendukung penyelenggaraan program.
Collaborative Process	*Commitmen to the process*	Terdapat komitmen antara seluruh aktor yang terlibat, baik penyelenggara, pemilik sistem elektronik, maupun masyarakat selaku pengidentifkasi dan/atau pemberi rekomendasi keamanan siber.
	Trust building	Membangun kepercayaan antar seluruh aktor yang terlibat
	Internal and external relationship	Adanya komunikasi yang intens baik secara internal, dan/atau eksternal organisasi untuk menciptakan keberlangsungan proses kolaborasi
	Consensus building	Ruang lingkup pekerjaan sesuai dengan apa yang disepakati sejak awal penyelenggaraan program
	Knowledge management	Adanya pengaturan pengetahuan yang telah didapat dan dibagikan kembali ke seluruh pihak yang terlibat

Dimensi	Sub Dimensi	Indikator
Equity Outcomes	*Multiple investment sources*	Adanya investasi dari berbagai pihak yang mendukung penyelenggaraan program, seperti kontribusi pemberian apresiasi terhadap masyrakat yang menjadi pengidentifikasi dan/atau pemberi rekomendasi keamanan.
	Accountability	Adanya transparansi dalam penyelenggaraan program yang dilakukan oleh entitas yang terlibat sebagai bentuk pertanggungjawaban
	Discoure and practice	Adanya hasil yang sesuai dengan tujuan awal kolaborasi, yakti hasil identifikasi kerentanan dan/atau rekomendasi pengamanan

Lampiran 2
Transkrip Wawancara 1

Ketua Tim ITSA Direktorat Operasi Keamanan Siber

Narasumber : Taufik Nurhidayat, S.ST
Jabatan : Ketua Tim IT *Security Assessment*, Direktorat Operasi Keamanan Siber
Unit Kerja : Direktorat Operasi Keamanan Siber, Deputi II BSSN
Tanggal : 5 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Bagaimana Tim ITSA dalam melibatkan Personilnya pada program Identifikasi Kerentanan dan Proteksi Secara Sukarela, terutama dalam konteks identifikasi kerentanan aplikasi SPBE? Apakah dengan keterlibatan tersebut akan memperkaya pandangan dan pengetahuan, sehingga dapat menjadi solusi atas keamanan siber di sektor pemerintahan?**

   Jawaban:

   Keterlibatan Tim dalam penyelenggaraan program Identifikasi Kerentanan dan Proteksi secara Sukarela ini memang didasari oleh komitmen bersama antara staf bersama pimpinan di BSSN. Hal ini dipengaruhi juga adanya sejumlah kondisi seperti munculnya banyak permintaan layanan ITSA dari stakeholder, keterbatasan sumber daya yang dimiliki BSSN untuk mengakomodir seluruh permintaan, serta adanya potensi pelibatan sumber daya di luar BSSN dari kalangan komunitas, Pegiat keamanan siber dan pihak lainnya untuk dapat terlibat dalam kegiatan identifikasi kerenanan. Selanjutnya secara spesifik program identifikasi kerentanan dan proteksi secara sukarela masih selaras dengan visi-misi BSSN terutama dalam hal menumbuh kembangkan talenta keamanan siber di luar BSSN.

   Adapun upaya yang telah dilakukan oleh Tim ITSA BSSN secara bersama-sama dengan pihak-pihak terkait di BSSN antara lain:

a. Penyiapan Sumber Daya Manusia

Secara Internal SDM di Tim ITSA telah mempersiapkan kemampuan di bidang identifikasi kerentanan guna mendukung pelaksanaan program Identifikasi Kerentanan dan proteksi secara sukarela. Adapun peran Tim ITSA yang menguasa Identifikasi kerentanan dapat membantu dalam sebagai verifikator terhadap laporan identifikasi kerentanan yang masuk pada saat program berjalan. Hal ini sebagaimana tertuang dalam Peraturan Kepala BSSN tentang program ini, BSSN menempatkan diri sebagai koordinator, sehingga tidak dapat terlibat langsung dalam proses identifikasi.

Dengan melihat potensi kedepan sangat besar, Tim ITSA juga telah berkolaborasi dengan pihak-pihak di luar Tim, sehingga kita juga sudah dapat menambah SDM, dan sangat memungkinkan untuk dilaksanakan dan ini juga telah dikomunikasikan kepada pimpinan. Dan juga melihat juga cakupan pekerjaan, sehingga resource perlu disesuaikan.

Secara Eksternal, Tim ITSA bersama tim lain di BSSN juga telah komunitas / Pegiat keamanan sinber, dengan melakukan pendekatan kepada komunitas secara format / informal (kedekatan), secara formal melakukan pendekatan secaui unit kerja pembinaan SDM Siber (D41). Pendekatan tersebut masih kita *maintenance*, baik kegiatan bersama temen2 komunitas, baik kegiatan werbinar, seminar, dabhak kegiatan IK. Untuk menjaga hubungan, kita jg sudah membuat grup chat telegram, sbg upaya akomodir mereka.

b. Penyiapan Proses / Tata Kelola

Dalam menjalankan kolaborasi penting untuk memperhatikan aturan yang dijadikan pedoman. Oleh karena itu, Tim ITSA terlibat juga dalam penyusunan Peraturan Kepala tentang pelaksanaan program IK dan Prokteksi ini, adapun semua ketentuan yang nantinya digunakan sebagai acuan sudah masuk ke masuk ke Perka tersebut. Dengan demikian diharapkan dapat membantu dalam penyelenggaraan program IK dan Prokteksi. Apabila dalam pelaksanaan membutuhkan hal-hal yang lebih detail, kami bersama Tim Program juga telah menyusun juknis, SOP, dan semua instrumen tersebut juga perlu disimulasikan mulai aturan main, dan

bagaimana peran dari masing-masing pihak yang terlibat. Jangan sampai ada hal-hal yang terlewat, dan mengganggua jalannya kegiatan. Baik dari prosedur yang dilewatkan, ataupun administrasi kegiatan seperti penandatangan perjanjian kerjasama seperti NDA, danan harapanya tidak ada pihak yang melanggar hukum.

c. Penyiapan Teknologi

Tim ITSA bersama tim penyusun program juga telah mengembangkan platform Identifikasi Kerentanan dan Proteksi yang dapat digunakan oleh seluruh pihak mulai dari BSSN, PSE Lingkup Publik, maupun Pegiat keamanan siber seperti Bug hunter. Namun dalam penyelenggaraan ini akan lebih baik jika ke depannya dapat dimanfaatkan oleh entitas lain yang bertugas sebagai tim pengawas.

2. Apa tujuan bersama yang ingin dicapai oleh Tim ITSA melalui program ini, khususnya dalam meningkatkan keamanan aplikasi SPBE melalui kegiatan identifikasi kerentanan?

Jawaban:

Berangkat dari tugas pokok dan fungsi BSSN, yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber. Dalam meningkatkan keamanan SPBE, BSSN perlu mengkolaborasikan seluruh stakeholder di Indonesia tidak hanya entitas pemerintah, industri, akademisi. Namun juga entitas komunitasi perlu dirangkul dalam rangka kolaborasi.

Sejalan dengan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Isber Nasional dan Manajemen Krisis Siber. BSSN dapat bergerak dan berkolaborasi dalam Quadhelix stakeholder. Quad Helix yang dimaksud meliputi unsur pemerintah, pelaku bisnis, akademisi, seta masyarakat atau komunitas. Keempat pemangku kepentingan tersebut dilibatkan sebagai upaya mendukung strategi keamanan siber nasional.

Kemudiaan setiap pemerintah, dalam menjalankan tugasnya tentunya akan menilai dan mengukur, berapa *outcome* yang berkaitan langsung tentang kesejahteraan yang dirasakan oleh masyarakat. Khusus untuk masyarakat

keamanan siber, melalui Program IK dan Proteksi ini diharapkan bisa dijadikan tempat mencari pengalaman, protofolio sabagai modal awal dalam terjun di bidang industri keamanan siber. Mereka bisa menerima, manfaatkan, dan mendapatkan pekerjaan sehingga dapat meningkat kesejahteraan mereka.

Keamanan siber juga disampaikan para ahli, Indonesia membutuhkan komponen cadangan. Komunitas kamsiber, sbg bentuk komcad, sehingga perlu dibina oleh BSSN. Jangan samapai digunakan untuk kriminilas, atau hal yang merugikan. Kita juga bisa menggali aspirasi dari kominitas, ini seperti apa. Terkait kamsiber yang diselenggarakan oleh BSSN, atau yang mengakomodir untuk mereka berkembang

3. **Adakah aturan awal yang dijelaskan kepada tim ITSA sebagai acuan dalam penyelenggaraan program Identifikasi Kerentanan dan Proteksi Secara Sukarela di konteks identifikasi kerentanan?**

   Jawaban:

   Dalam menjalankan kolaborasi penting untuk memperhatikan aturan yang dijadikan pedoman. Oleh karena itu, Tim ITSA terlibat juga dalam penyusunan Peraturan Kepala tentang pelaksanaan program IK dan Prokteksi ini, adapun semua ketentuan yang nantinya digunakan sebagai acuan sudah masuk ke masuk ke Perka tersebut. Dengan demikian diharapkan dapat membantu dalam penyelenggaraan program IK dan Prokteksi.

   Apabila dalam pelaksanaan membutuhkan hal-hal yang lebih detail, kami bersama Tim Program juga telah menyusun juknis, SOP, dan semua instrumen tersebut juga perlu disimulasikan mulai aturan main, dan bagaimana peran dari masing-masing pihak yang terlibat. Jangan sampai ada hal-hal yang terlewat, dan mengganggua jalannya kegiatan. Baik dari prosedur yang dilewatkan, ataupun administrasi kegiatan seperti penandatangan perjanjian kerjasama seperti NDA, dan harapanya tidak ada pihak yang melanggar hukum.

4. **Sebagai Ketua Tim ITSA, bagaimana Anda mendukung dan memfasilitasi anggota tim dalam menjalankan program ini, dengan tidak meninggalkan tugas dan fungsi Tim ITSA sehari-hari?**

Jawaban:

Secara Internal SDM di Tim ITSA telah mempersiapkan kemampuan di bidang identifikasi kerentanan guna mendukung pelaksanaan program Identifikasi Kerentanan dan proteksi secara sukarela. Adapun peran Tim ITSA yang menguasa Identifikasi kerentanan dapat membantu dalam sebagai verifikator terhadap laporan identifikasi kerentanan yang masuk pada saat program berjalan. Hal ini sebagaimana tertuang dalam Peraturan Kepala BSSN tentang program ini, BSSN menempatkan diri sebagai koordinator, sehingga tidak dapat terlibat langsung dalam proses identifikasi.

Dengan melihat potensi kedepan sangat besar, Tim ITSA juga telah berkolaborasi dengan pihak-pihak di luar Tim, sehingga kita juga sudah dapat menambah SDM, dan sangat memungkinkan untuk dilaksanakan dan ini juga telah dikomunikasikan kepada pimpinan. Dan juga melihat juga cakupan pekerjaan, sehingga resource perlu disesuaikan.

5. **Bagaimana persepsi interdependensi antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber dalam menjalankan program ini? Bagaimana Anda melihat peran tim ITSA dalam mencapai tujuan kolaboratif, terutama dalam konteks identifikasi kerentanan?**

   Jawaban:

   Persepsi interdependensi antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber menunjukkan hubungan ketergantunganm dimana terdapat adanya kebutuhan IK dari PSE, atas kebutuhan mereka. Di sisi lain mereka tidak punya resource, sehingga munculnya entitas baru (komunitas) sebagai peluang untuk membantu PSE dalam melakukan identifikasi kerentanan melalui program ini.

   Selanjutnya bagaimana, adanya hubungan keterkaitam, timbal balik dari masing-masing pihak, diantaranya seperti:

   a. PSE Lingkup Publik akan mendapatkan layanan IK dan proteksi akibat kurang resource dari PSE itu sendiri.
   b. Bug hunter juga membutuhkan portofolio sebagai modal mencari pekerjaan atau kegiatan lain seperti peningkatan kapabilitas, sertifikasi keahlian di bidang keamanan siber. Selain itu adanya rasa prestis / pernghargaan yang

akui dan diterbitkan oleh BSSN yang harapannya akan meningkatkan nilai pada saat mencari pekerjaan. Dimana BSSN merupakan lembaga pemerintah yang bergerak dan membina bidang keamanan siber di Indonesia.

c. BSSN juga menjadi pihak yang membutuhkan pihak lainnya dalam meningkatkan ekosistem keamanan siber di Indonesia. BSSN menajdi pihak yang dapat menghubungkan antara PSE Lingkup Publik dan masyarakat. Dimana ketika bug hunter atau Pegiat keamanan siber melakukan komunikasi / hubunan langsung dengan PSE Lingkup Publik, belum sepenuhnya saling percaya bahkana bisa jadi tidak percaya. Sehingga kehadiran BSSN menjadi perantara yang baik bagi kedua belah pihak.

6. **Bagaimana Tim ITSA membangun dan mempertahankan kepercayaan dalam tim internal dan kolaborasi eksternal khususnya hubungan antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber dalam konteks identifikasi kerentanan?**

   Jawaban:

   Untuk membangun kepercayaan dalam konteks Identifikasi kerentanan, secara internal Tim ITSA telah memiliki pemahaman yang akan tupoksi dan tanggunjawab masing-masing personil di Tim ITSA. Dengan berbekal kemampuan yang dimiliki oleh personil Tim ITSA yang mana secara keseluruhan adalah Lulusan dari Sekolah Tinggi Sandi Negara atau Politeknik Siber dan Sandi Negara. Sehingga tim telah dibekali dengan kemampuan yang cukup, sehingga kami percaya akan seluruh tim yang ada, dan dapat menjalankan tugas dan tanggung jawab sesuai kebutuhan organisasi.

   Selanjutnya secara ekternal dengan pihak-pihak lain seperti PSE Lingkup Publik, dan Pegiat Keamanan Siber, Tim juga telah menjaga hubungan yang baik dengan PSE Lingkup Publik telah menjalin hubungan kerjasama di bidang identifikasi melalui layanan IT *Security Assessment*. Kemudian juga telah menjalin hubungan dengan Pegiat Keamanan Siber, kami telah membuat *channel* dan *group* telegram secara khusus yang dapat digunakan berkomunikasi dengan mereka. Selain itu, BSSN juga telah menyelenggarakan

serangkaian pilot project, dan webinar yang berkaitan dengan pelaksanaan program ini.

7. **Bagaimana komitmen Tim ITSA terhadap proses kolaboratif dalam program ini?**

   Jawaban

   Komitmen kami mendukung 100%, hal ini bisa dilihat dari :

   a. Timeline penyusunan regulasi yang sangat singkat. Inisiasi penyusunan ini dimulai dari awal 2023, dan akhirnya bisa selesai 2023 serta ditetapkan oleh Kepala BSSN.
   b. Tim Itsa bersama pihak-pihak terkait di BSSN juga telah menyiapkan sumber daya, seperti SDM yang mengawaki, Platform / Aplikasi yang digunakan dalam penyelenggaraan program, dan tentunya yang mengawaki program ini tidak main-main. Semua pihak telah mendedikasikan untuk terlaksananya program ini.
   c. Pada Level Pimpinan, kita juga sudah memperjuangkan dari level bawah hingga pucuk pimpinan, dan semua sudah setujui.
   d. BSSN juga masih menjaga atau me-*maintance* hubungan baik dengan Bug Hunter / Komunitas / Pegiat Keamanan Siber dan PSE Lingkup Publik

8. **Bagaimana Tim ITSA menjaga hubungan internal dan eksternal untuk mendukung keberlangsungan proses kolaborasi?**

   Jawaban:

   Untuk menjaga hubungan yang baik secara internal Tim ITSA telah memiliki pemahaman yang akan tupoksi dan tanggunjawan masing-masing personil di Tim ITSA. Dengan berbekal kemampuan yang dimiliki oleh personil Tim ITSA yang mana secara keseluruhan adalah Lulusan dari Sekolah Tinggi Sandi Negara atau Politeknik Siber dan Sandi Negara. Sehingga tim telah dibekali dengan kemampuan yang cukup, sehingga kami percaya akan seluruh tim yang ada, dan dapat menjalankan tugas dan tanggung jawab sesuai kebutuhan organisasi.

   Selanjutnya secara ekternal dengan pihak-pihak lain seperti PSE Lingkup Publik, dan Pegiat Keamanan Siber, Tim ITSA juga telah membina hubungan

yang baik. Tim ITSA dengan PSE Lingkup Publik telah menjalin hubungan kerjasama di bidang identifikasi melalui layanan IT Security Assessment. Dan dengan Pegiat Keamanan Siber, kami telah membuat channel dan group khusus yang dapat digunakan berkomunikasi dengan mereka. Selain itu, Tim ITSA bersama BSSN juga telah menyelenggarakan serangkaian pilot project, dan webinar yang berkaitan dengan pelaksanaan program.

9. **Bagaimana Tim ITSA berpartisipasi dalam mencapai konsensus dalam menetapkan ruang lingkup pekerjaan dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawaban:

   Secara teknis Tim ITSA akan memberikan masukan dan melakukan kontrol terhadap pelaksaan pengujian sistem elektronik berdasarkan ruang lingkup yang telah diusulkan PSE Lingkup publik dan telah ditetapkan dalam program yang berjalan. Sehingga ketika terjadi pengujian sistem elektronik di luar ruang lingkup pengujian yang dilakukan oleh peserta pengidentifikasi kerentanan. Maka hal ini akan menjadikan laporan yang nantinya dikirimkan ke penyelenggara program dapat dinyatakan out-of-scoope dengan nilai minus, dan berdampak terhadap nilai akumulasi peserta tersebut.

   Dengan demikian, seluruh pihak yang terlibat dalam program harus benar-benar memperhatikan apa yang menjadi lingkup pekerjaan dari program yang telah ditetapkan.

10. **Bagaimana Tim ITSA mengelola pengetahuan yang didapat selama proses kolaborasi, terutama informasi kerentanan dari hasil pengujian?**

    Jawaban:

    Untuk mendapatkan pengetahuan yang cukup, kami akan menjalankan beberapa program melalui paltform dengan beberapa pilot project terkait penyelenggaraan program ini. Tentunya dalam jalannya akan ada evaluasi. Sehingga harapnya akan menjalankan secara efektif dan efisien. Evaluasi akan tetap dijalankan.

Ketika mendapatkan data kerentanan / statistik dan kumpulan data-data tersebut. Tidak hanya akan diolah menjadi himabuan keamanan, tapi ke depan akan didalami lebih lanjut sbg profile kerentanan berdasarkan sektor IIV.
Selanjutnya data yag dioleh dpt dijadikan rujukan untuk sektor-sektor tertentu. Namun demikian, data-data yang diproses merupakan data-data general untuk konsumsi publik atau data-data yang dijadikan sebagai bahan pengambilan keputusan sebagai upaya transpormasi digial.

11. **Bagaimana pendapat Anda terkait alokasi apresiasi terhadap peserta yang berprestasi dalam program ini?**

    Jawaban:

    Terkait apresiasi yang dialokasikan terhadap peserta yang berprestasi adalah sesuatu hal yang penting. Mengingat ini adalah salah satu faktor pendorong bagi para Pegiat keamanan siber untuk terlibat dan ingin mengikuti program ini. Selain itu apresiasi juga menandakan di level mana peserta tersebut dalam program ini. Semakin tinggi posisi peringkat yang didapatkan dari nilai-nilai pelaporannya, maka akan semakin besar juga peluang mendapatkan apresiasi yang bernilai tinggai bagi para peserta. Sehingga alokasi apresiasi pada program identifikasi kerentanan dan proteksi secara sukarela ini menjadi hal yang bisa dikatakan mutlak ada. Namun kembali lagi, ke prinsip dasar dari program, yaitu secara sukarela. Artinya peserta secara sadar dan rela berkenan untuk ikut dalam pelaksaan program ini, apapun bentuk apresiasinya. Namun BSSN juga perlu menetapkan standar yang tinggi, untuk menggaet para Pegiat keamanan siber agar berkontribusi dalam peningkatan keamanan siber di Indonesia.

12. **Apa pandangan Tim ITSA tentang akuntabilitas dalam penyelenggaraan program, terutama dalam konteks identifikasi kerentanan? Di sisi lain memungkinkan pengidentifikasi kerentanan tidak melaporkan seluruh kerentanan pada sistem elektronik yang diuji.**

    Jawaban:

    Dengan adanya mekanisme yang telah ditetapkan, semua entitas sudah diikat dengan perjanjian yang dapat mengikat, sehingga menjadi pembatas bagi hal-

hal yang tidak diinginkan. Namun dalam pelaksanaanya, memang seringkali memang terjadi hal-hal yang tidak diinginkan. Namun sekali lagi, adanya aturan bisa menjadi pembatas dan pengatur keselurahan entitas. Namun jika ada entitas ke 4 yg menjadi pengawas bisa meningkatkan penyelenggaran identifikasi kerentanan dan proteksi ini, seperti Aparat Penegak Hukum, asosiasi dkk.

13. **Bagaimana Tim ITSA menilai keberhasilan program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Adakah suatu indikator khusus dari sudut pandang tim ITSA?**

Jawaban:

Harapanya kami bisa berhasil, kita sudah melakukan riset untuk mebangun kegiatan ini. Paling tidak bisa menginisasi kegiatan lain, tidak hanya di sektor pemeritnah, tapi bisa juga di sektor lain. Selain itu, program ini juga dapat menjadi inisiasi untuk kegiatan lain, seperti pembinaan komunitas, dan pembinaan ekosistem siber lainnya.

Bisa jadi disektor industri bisa tumbuh kembang, terutama sektor industri keamanan siber, dan menjadikan pelaku insustri lebih bervariatif mulai dari alat yang diperjualbelikan, dan tidak hanya pihak itu-itu saja yang bermain di indusri ini.

Untuk menilai keberhasilan program ini, tim itsa juga telah menetapkan indikator khusus, seperti:

a. Timeline kegiatan, yang dibreakdown per thn/ smester, dengan target meningkat dalam kurun waktu tertenu misal thn pertama sekian bug hunter, sekian sistem elektronik, dan sekian PSE lingkup publik, dst.
b. VVIP masih lekat dengan BSSN, mulai dari pembiyaan dan penyelenggaraan. Kedepan memungkinkan bisa jadi program secara mandiri, terutama dari hal pembiayaan. Sehingga juga berdampak pada kompensasi yang lebih banyak untuk para Pegiat keamanan siber. Para pelaku industri keamanan siber juga berpeluang dalam memberikan dukungan pelaksanaan program ini.

Lampiran 3
Transkrip Wawancara 2

Ketua Tim Proteksi Direktorat Operasi Keamanan Siber

Narasumber	:	Indra Adi Putra, S.ST., M.M
Jabatan	:	Ketua Tim Proteksi, Direktorat Operasi Keamanan Siber
Unit Kerja	:	Direktorat Operasi Keamanan Siber, Deputi II BSSN
Tanggal	:	8 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Bagaimana keterlibatan Tim Proteksi terlibat dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Apakah dengan keterlibatan tersebut akan memperkaya pandangan dan pengetahuan, sehingga dapat menjadi solusi atas keamanan siber di sektor pemerintahan?**

   Jawaban:

   Tim Proteksi terlibat dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela dengan menjadi penyelenggara program tersebut. Melalui keterlibatan ini, kami memberikan kontribusi dalam menganalisis dan mengidentifikasi kerentanan pada sistem elektronik pemerintahan. Keterlibatan ini diharapkan dapat memperkaya pandangan dan pengetahuan kami dalam memahami berbagai ancaman keamanan siber yang mungkin terjadi di sektor pemerintahan, sehingga dapat memberikan solusi yang lebih efektif.

2. **Sebagai Ketua Tim Proteksi, bagaimana Anda mendukung dan memfasilitasi anggota tim dalam menjalankan program ini, dengan tidak meninggalkan tugas dan fungsi Tim Proteksi sehari-hari?**

   Jawaban:

   Sebagai Ketua Tim Proteksi, saya mendukung anggota tim dengan memberikan bimbingan dan sumber daya yang dibutuhkan untuk menjalankan program ini. Fasilitasi ini dilakukan tanpa meninggalkan tugas dan fungsi Tim Proteksi

sehari-hari, dengan memastikan bahwa anggota tim dapat melaksanakan tugasnya dengan efisien dan efektif.

3. **Apa tujuan bersama yang ingin dicapai oleh Tim Proteksi melalui program ini, khususnya dalam meningkatkan keamanan aplikasi SPBE melalui kegiatan identifikasi kerentanan?**

   Jawaban:

   Tujuan bersama yang ingin dicapai adalah meningkatkan keamanan aplikasi SPBE dengan melakukan identifikasi kerentanan, dan memastikan seluruh kerentanan dapat diremidiasi dan diperbaiki sebagaimana mestinya. Dengan demikian, dapat memberikan jaminan akan kerahasiaan, integritas dan ketersediaan sistem elektronik pemerintahan, menciptakan lingkungan yang lebih aman dan terlindungi dari ancaman siber

4. **Apakah ada aturan awal yang dijelaskan kepada anggota Tim Proteksi sebagai panduan dalam melaksanakan program Identifikasi Kerentanan dan Proteksi Secara Sukarela di konteks perlindungan sistem elektronik?**

   Jawaban:

   Aturan yang dijadikan rujukan dalam penyelenggaraan program ini adalah Peraturan Kepala Badan Siber Dan Sandi Negara Nomor 5 Tahun 2023 tentang Penyelenggaraan Program Identifikasi Kerentanan Dan Proteksi Secara Sukarela. Di dalam aturan tersebut, telah diatur ruang lingkup, hak, kewajiban, apresiasi, dan sanksi yang diberlakukan bagi peserta kegiatan.

5. **Bagaimana persepsi interdependensi antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber dalam menjalankan program ini? Bagaimana Anda melihat peran tim Proteksi dalam mencapai tujuan kolaboratif, terutama dalam konteks proteksi sistem elektronik?**

   Jawaban:

   Persepsi interdependensi antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber sangat penting dalam menjalankan program ini. Tim Proteksi melihat dirinya sebagai elemen kunci dalam mencapai tujuan kolaboratif dengan memberikan kontribusi pada proteksi sistem elektronik, berkoordinasi

secara efektif dengan pihak terkait. BSSN berupaya untuk merangkul seluruh pihak untuk mengamankan sistem elektronik milik pemerintah. Kolaborasi ini dapat diwujudkan dari sisi Pegiat keamanan siber untuk melakukan pengujian kerentanan serta dari sisi PSE Lingkup Publik untuk melakukan penguatan sistem elektronik.

6. **Melihat sudah tersedianya standar teknis dan prosedur keamanan aplikasi SPBE, bagaimana keterkaitan dengan program ini?**

   Jawaban:

   Program ini dimaksudkan sebagai upaya percepatan implementasi atas standar teknis dan prosedur keamanan aplikasi SPBE yang telah ada. Standar teknis dan prosedur keamanan aplikasi SPBE sangat relevan dengan program ini. Tim Proteksi memastikan bahwa identifikasi kerentanan dan rekomendasi pengamanan yang dihasilkan sejalan dengan standar keamanan yang telah ditetapkan.

7. **Bagaimana upaya Tim Proteksi untuk membangun dan menjaga kepercayaan terhadap seluruh entitasi yang terlibat dalam penyelenggaraan program identifikasi kerentanan dan proteksi secara sukarela?**

   Jawaban:

   Tim Proteksi telah mengupayakan dalam membangun dan menjaga kepercayaan melibatkan transparansi dalam pelaksanaan program, komunikasi terbuka, dan konsistensi dalam penanganan temuan keamanan. Hal ini bertujuan untuk memastikan bahwa seluruh entitas yang terlibat merasa yakin dengan integritas dan tujuan dari program ini.

8. **Sejauh mana Tim Proteksi berkomitmen pada proses kolaboratif melalui program tersebut, kaitannya melindungi sistem elektronik atas ancaman siber yang semakin beragam?**

   Jawaban:

Tim Proteksi berkomitmen penuh pada proses kolaboratif melalui program ini, mengenali bahwa melindungi sistem elektronik dari ancaman siber memerlukan sinergi antara pemerintah dan masyarakat. Komitmen ini tercermin dalam partisipasi aktif dalam identifikasi kerentanan dan penerapan rekomendasi keamanan.

9. **Dalam menjalankan program kolaborasi, tentunya membutuhkan komitmen bersama dan hubungan yang baik antar semua aktor yang terlibat. Bagaimana upaya yang dilakukan Tim Proteksi, baik internal maupun eksternal untuk mendukung kelangsungan proses kolaborasi ini? Seperti upaya dalam kesepakatan ruang lingkup pekerjaan, aturan main, syarat dan ketentuan program terutama terkait perlindungan sistem elektronik?**

   Jawaban:

   Tim Proteksi berupaya untuk menjalin hubungan yang baik dengan semua pihak baik kepada PSE Lingkup Publik maupun Pegiat keamanan siber. Dari sisi PSE Lingkup Publik, Tim Proteksi telah menyediakan form yang dapat diisi oleh PSE Lingkup Publik terkait kesepakatan aplikasi yang akan diuji misalnya berapa banyak aplikasi, metode pengujian, serta *environment* aplikasi. Dari sisi Pegiat keamanan siber, BSSN berupaya untuk melakukan pengelolaan terhadap komunitas keamanan siber di luar sana agar dapat diberdayakan untuk kegiatan yang positif.

10. **Bagaimana strategi Tim Proteksi mengelola pengetahuan yang diperoleh selama proses kolaborasi, terutama dalam konteks bagaimana melakukan proteksi sistem elektronik berdasarkan rekomendasi pengamanan?**

    Jawaban:

    Strategi Tim Proteksi dalam mengelola pengetahuan melibatkan dokumentasi yang cermat, penyimpanan informasi yang aman, dan penggunaan database pengetahuan untuk menyimpan rekomendasi keamanan dan pengalaman yang diperoleh selama proses kolaborasi.

11. **Bagaimana pendapat Anda terkait alokasi apresiasi terhadap peserta yang berprestasi dalam program ini?**

    Jawaban:

    Kami memberikan apresiasi kepada peserta yang berprestasi dalam program ini melalui pengakuan publik, sertifikat penghargaan, atau mungkin insentif lainnya. Hal ini bertujuan untuk mendorong semangat dan dedikasi dalam meningkatkan keamanan sistem elektronik. Selain itu, kami juga memberikan kesempatan bagi PSE Lingkup Publik untuk berpartisipasi dalam pemberian apresiasi kepada peserta yang berprestasi pada program ini

12. **Apa pandangan Tim Proteksi tentang akuntabilitas dalam penyelenggaraan program, terutama dalam konteks Proteksi?**

    Jawaban:

    Tim Proteksi melihat akuntabilitas sebagai landasan penting dalam penyelenggaraan program ini. Setiap tindakan dan keputusan harus dapat dipertanggungjawabkan, sehingga dapat memastikan integritas dan keberlanjutan program.

13. **Bagaimana Tim Proteksi menilai keberhasilan program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Adakah suatu indikator khusus dari sudut pandang tim Proteksi?**

    Jawaban:

    Indikator utama dari keberhasilan program ini adalah menurunnya kasus serangan siber di Indonesia. Selain itu, indikator lain yang mendukung keberhasilan program Identifikasi Kerentanan dan Proteksi Secara Sukarela dinilai oleh Tim Proteksi melalui indikator seperti jumlah kerentanan yang berhasil diidentifikasi dan diperbaiki, tingkat kepatuhan terhadap standar keamanan, dan dampak positif terhadap keamanan sistem elektronik pemerintahan. Evaluasi ini memastikan bahwa program memberikan nilai tambah yang signifikan dalam melindungi aset informasi pemerintah.

Lampiran 4
Transkrip Wawancara 3

Pegiat Keamanan Siber

Narasumber : R. Setyawan
Jabatan : Pegiat Keamanan Siber
Tanggal : 7 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Sebagai Pegiat keamanan siber, apakah anda mengetahui program sejenis ini, dan bagaimana pendapat anda mengenai program yang diterbitkan oleh BSSN? Bagaimana mekanisme Pegiat keamanan siber untuk berpartisipasi dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawab:

   Saya sangat mengetahui program sejenis ini dan melihatnya sebagai langkah positif dari BSSN. Program Identifikasi Kerentanan dan Proteksi Secara Sukarela memberikan kesempatan bagi saya untuk berkontribusi langsung dalam meningkatkan keamanan aplikasi pemerintah. Adapun mekanisme untuk berpartisipasi biasanya melibatkan pendaftaran melalui platform atau kanal resmi yang disediakan oleh penyelenggara, diikuti dengan pengujian keamanan yang sesuai dengan aturan yang telah ditetapkan. Namun demikian perlu meningkatkan literasi dan publikasi terkait program ini, sehingga para pemilik sistem, komunitas dan masyarakat secara umum dapat mengetahui dan lebih banyak lagi yang berpartisipasi.

2. **Menurut pandangan Anda sebagai Pegiat keamanan siber, apa yang mendasari tujuan bersama dalam meningkatkan keamanan aplikasi pemerintah melalui program ini?**

   Jawab:

   Tujuan bersama yang mendasari adalah meningkatkan keamanan aplikasi pemerintah. Selain itu melalui program ini didorong oleh kebutuhan akan

perlindungan yang lebih baik terhadap sistem elektronik. Namun tidak semua Pegiat keamanan siber sudah memahami ini. Sebagai contoh para pencari bug / kerentanan yang masih muda seperti dikalangan siswa SMP, dan SMA perlu diberikan edukasi yang baik, sehingga mereka benar-benar paham bahwa pemerintah memiliki program yang serius. Saat ini para hacker baik di usia muda masih berada di kondisi mencari jati diri, mencari eksistensi, mencari ketenaran yang mana sering dilakukan dengan cara yang tidak baik seperti melakukan serangan web defacement di situs-situs pemerintah dan di situ memberikan beberapa kode, nama-nama hackernya.

Dengan demikian, Kolaborasi antara pemerintah dan Pegiat keamanan siber tidak hanya membantu mengidentifikasi kerentanan yang mungkin tidak terdeteksi secara internal, memperkuat lapisan keamanan, dan menciptakan ekosistem keamanan siber yang lebih tangguh. Namun juga sebagai wadah bagi pembinaan kepada masyarakat terutama kepada mereka-meraka yang memiki kemampuan di bidang keamanan siber untuk tidak menyalahgunakannya.

3. **Bagaimana respon Anda terhadap inisiatif BSSN terhadap program Identifikasi Kerentanan dan Proteksi Secara Sukarela yang akan segera dimulai?**

   Jawab:

   Saya menyambut baik inisiatif BSSN terhadap program Identifikasi Kerentanan dan Proteksi Secara Sukarela. Hal ini mencerminkan komitmen pemerintah dalam menghadapi tantangan keamanan siber dengan melibatkan para ahli dari masyarakat.

   Namun demikian perlu meningkatkan literasi dan publikasi terkait program ini, sehingga para pemilik sistem, komunitas dan masyarakat secara umum dapat mengetahui dan lebih banyak lagi yang berpartisipasi, serta apresiasi yang tepat sebagai nilai jual lebih.

4. **Berdasarkan pengalaman Anda, Apakah Anda memiliki pengetahuan tentang aturan awal (*preliminary rules*) yang dijadikan acuan dalam mengikuti program serupa Identifikasi Kerentanan dan/atau Proteksi Secara Sukarela?**

   Jawab:

   Aturan awal (*preliminary rules*) biasanya dijelaskan oleh penyelenggara program, mencakup pedoman etika, batasan pengujian, dan mekanisme pelaporan hasil temuan. Sebagai Pegiat keamanan siber, memahami aturan ini penting sebelum berpartisipasi dalam program.

5. **Dalam melakukan kolaborasi pemerintah dan masyarakat, Bagaimana Anda sebagai Pegiat keamanan siber memandang pentingnya hubungan saling ketergantungan antara seluruh pihak yang terlibat dalam program ini?**

   Jawab:

   Hubungan saling ketergantungan antara semua pihak terlibat sangat penting dalam program ini. Saya memandang pentingnya kolaborasi untuk memahami secara menyeluruh ancaman dan kerentanan yang ada, serta merumuskan solusi yang efektif.

   Selain itu dari sisi Pegiat keamanan siber kita memandang perlunya adanya langkah kongkrit yang diambil para pemilik sistem yang berasal dari instansi pemerintah. Dari beberapa berdiskusi dengan para Pegiat yang melaporkan kerentanan kepada instansi-instansi tersebut hanya mendapatkan respon "**baik terimakasih kasih mas**" namun tidak melakukan aksi yang tepat, sehingga kerentanan sistem tersebut tidak benar-benar ditutup secara cepat. Hal ini tentunya akan mengkhawatirkan keadaan sistem tersebut dan diakhirnya nanti mungkin akan berdampak terhadap citra organisasi. Ini kaitannya juga dengan wibawa pimpinan di organisasi tersebut. Dari pengalaman tidak sedikit Kepala Unit TIK yang belum memiliki kesadaran keamanan siber yang baik.

   Penting untuk melihat peran masing-masing lagi sesuai tugas dan tanggung jawab pada proses kolaborasi ini. Sebagai Pegiat kami juga ingin membantu pemerintah untuk meningkatkan keamanan sibernya.

6. **Apakah Anda memberikan investasi awal untuk mengikuti program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Seperti biaya pendaftaran, atau investasi dalam bentuk lain. Berkenan anda dapat menjelaskan secara lengkap.**

   Jawab:

   Sebagai Pegiat keamanan siber, investasi awal seperti biaya pendaftaran biasanya dianggap sebagai investasi dalam pengembangan keamanan siber dan keberlanjutan program ini. Selain itu, saya juga telah mengembangkan kompetensi diri dengan mengikuti pelatihan serta sertifikasi terkait keamanan siber. Namun, seiring dengan kontribusi yang diberikan, apresiasi dalam bentuk uang tunai, souvenir, atau sertifikat juga dapat diharapkan. Hal ini akan menjadi penyemangat bagi kami untuk berpartisipasi pada program-program seperti ini. terlebih lagi program identifikasi kerentanan yang sifatnya sukarela, jika tidak memiliki apresiasi yang jelas akan kurang diminati di kalangan Pegiat keamanan siber yang sudah memiliki jam terbang tinggi. Mereka akan mempertimbangkan program-program yang menghasilkan bounty / apresiasi yang besar.

7. **Untuk menjamin terselenggaranya program Identifikasi kerentanan dan Proteksi Secara Sukarela dibutuhkan komitmen bersama antar seluruh entitias yang terlibat, baik dari penyelenggara, pemilik sistem elektronik, dan para Pegiat keamanan siber.**

   Apakah Anda memiliki komitmen terhadap proses kolaboratif dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?

   Jawab:

   Jika program ini berjalan, maka Saya memiliki komitmen penuh terhadap proses kolaboratif dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela. Kolaborasi ini penting untuk mencapai tujuan bersama dalam meningkatkan keamanan sistem elektronik pemerintah. Bagi kami yang memiliki kepedulian terhadap kondisi ekosistem keamanan siber di Indonesia membutuhkan program-program seperti ini dan tentunya melalui koordinasi dari pemerintah. Namun demikian perlu meningkatkan literasi dan publikasi

terkait program ini, sehingga para pemilik sistem, komunitas dan masyarakat secara umum dapat mengetahui dan lebih banyak lagi yang berpartisipasi.

8. **Bagaimana Anda selaku Pegiat keamanan siber dapat membangun kepercayaan dengan seluruh aktor yang terlibat dalam program ini? Adakah klausul / prasyarat yang dapat dijadikan acuan?**

   Jawab:

   Saya berharap adanya upaya untuk membangun kepercayaan melibatkan transparansi, komunikasi terbuka, dan pemenuhan kewajiban yang diatur dalam aturan program. Klausul atau prasyarat tertentu dapat dijadikan acuan untuk memastikan integritas dan keamanan informasi. Dengan adanya hal tersebut dapat memperkuat pelaksanaan dan kepatuhan oleh pihak-pihak yang terlibat terhadap peraturan yang ada.

9. **Berdasarkan pengalaman Anda, apakah anda pernah bekerjasama dengan instansi pemerintah? Jika pernah, bagaimana anda menjaga hubungan tersebut jika dikaitkan dengan program yang ditetapkan oleh BSSN untuk mendukung keberlangsungan proses kolaborasi?**

   Jawab:

   Saya pernah bekerjasama dengan instansi pemerintah dalam program serupa. Untuk menjaga hubungan tersebut, komunikasi terbuka, penghormatan terhadap aturan program, dan pemahaman mendalam terhadap tujuan bersama sangat penting.

10. **Dalam melaksanakan identifikasi kerentanan dan/atau memberikan rekomendasi proteksi dibutuhkan ruang lingkup yang jelas dan tepat. Apakah anda selaku Pegiat keamanan siber dapat memutuskan bahwa anda sepakat dengan ruang lingkup pekerjaan dalam program yang diselenggarakan?**

    Jawab:

    Sebagai Pegiat keamanan siber, penting untuk memastikan bahwa ruang lingkup pekerjaan dalam program sesuai dengan keahlian dan kemampuan saya.

Keterlibatan dalam tahapan perencanaan dan definisi ruang lingkup dapat membantu untuk memastikan kesesuaian scope pekerjaan yang saya lakukan.

11. **Ketika anda mengikuti program Identifikasi kerentanan dan proteksi secara sukarela, tentunya mendapatkan berbagai informasi sensitif terkait kerentanan dan sistem elektronik terkait, dan memungkinkan mendapatkan informasi sensitif lainnya seperti data pribadi. Bagaimana Anda selaku Pegiat keamanan siber mengelola pengetahuan yang didapat selama proses kolaborasi?**

    Jawab:

    Pengelolaan pengetahuan melibatkan dokumentasi yang cermat, penyimpanan informasi yang aman, dan kepatuhan terhadap kebijakan privasi. Saya akan memastikan bahwa informasi sensitif dikelola dengan aman dan hanya diakses oleh pihak yang berwenang. Tentunya apabila data yang saya dapatkan dari sebuah celah kerentanan merupakan data sensitif, saya akan bertindak secara etis untuk tidak menyimpan, mempublikasikan, maupun membocorkan data tersebut sesuai dengan kesepakatan perjanjian yang telah saya tandatangani, biasanya ada dokumen perjanjian kerahasiaan seperti *Non-Dosclosure Agreement*.

12. **Dari program yang anda ikuti, apakah penyelenggara dan/atau pemilik sistem elektronik memberikan hak-hak apresiasi berdasarkan kontribusi anda ?**

    Jawab:

    Penyelenggara dan/atau pemilik sistem elektronik memberikan hak apresiasi berdasarkan kontribusi saya dalam bentuk penghargaan publik, sertifikat, atau imbalan lainnya.

13. **Jika dalam pelaksanaannya, Anda berhasil menemukan kerentanan lain terkait ruang lingkup pengujian pada media online sumber terbuka (*open source*) baik berupa dugaan kebocoran data, atau informasi sensitif lainnya. Apa langkah yang Anda ambil sebagai bentuk komitmen anda untuk menjadi Hacker Baik?**

    Jawab:

    Saya bersedia melaporkan temuan tambahan terkait keamanan pada media online sumber terbuka sebagai bentuk komitmen sebagai Hacker Baik. Hal ini dapat mempercepat dalam membantu pemilik sistem untuk melakukan tindakan reaktif dari temuan tersebut.

14. **Bagaimana Anda menilai program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil?**

    Jawab:

    Keberhasilan program Identifikasi Kerentanan dan Proteksi Secara Sukarela dapat diukur oleh sejauh mana kerentanan berhasil diidentifikasi dan diperbaiki, tingkat partisipasi Pegiat keamanan siber, dan dampak positif terhadap keamanan sistem elektronik pemerintah. Evaluasi ini dapat memberikan pandangan secara menyeluruh terhadap efektivitas program. Dengan demikian, harapannya dapat membawa keberhasilan pelaksanaan program ini.

Lampiran 5
Transkrip Wawancara 4

Pegiat Keamanan Siber

Narasumber : R. Sandya
Jabatan : Pegiat Keamanan Siber
Tanggal : 29 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Sebagai praktisi keamanan siber, apakah anda mengetahui program sejenis ini, dan bagaimana pendapat anda mengenai program yang diterbitkan oleh BSSN? Bagaimana mekanisme praktisi keamanan siber untuk berpartisipasi dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawab:

   Ya, beberapa program yang saya ketahui seperti Bugcrowd, dan Hacker One juga menyediakan program sukarela dengan hadiah berupa poin tidak hanya uang. Pada program tersebut partisipasi sangat mudah, mengisi formulir pendaftaran dan menyediakan informasi dasar mengenai diri kita untuk dilengkapi ketika sudah mendapatkan konfirmasi email pendaftaran.

2. **Menurut pandangan Anda sebagai praktisi keamanan siber, apa yang mendasari tujuan bersama dalam meningkatkan keamanan aplikasi pemerintah melalui program ini?**

   Jawab:

   Menurut saya pribadi, dasar dari kegiatan ini ialah adanya peningkatan atas kesadaran keamanan siber di Indonesia, apalagi setelah kita tahu kalau beberapa instansi mengalami kebocoran data, sebut saja yang paling heboh ialah ketika BPJS dan KPU mengalami kebocoran. Dari situ timbul juga motivasi saya untuk melakukan pengamanan sistem secara sukarela, terutama bagi Indonesia, karena data saya juga disimpan di Indonesia.

3. **Bagaimana respon Anda terhadap inisiatif BSSN terhadap program Identifikasi Kerentanan dan Proteksi Secara Sukarela yang akan segera dimulai?**

   Jawab:

   Saya sangat apresiasi niatan BSSN menciptakan program ini, ketika mendengar informasi mengenai program ini, saya sebagai masyarakat merasa diakui dengan disediakannya wadah bagi saya untuk menyalurkan niat baik saya.

4. **Berdasarkan pengalaman Anda, Apakah Anda memiliki pengetahuan tentang aturan awal (*preliminary rules*) yang dijadikan acuan dalam mengikuti program serupa Identifikasi Kerentanan dan/atau Proteksi Secara Sukarela?**

   Jawab:

   Ya, meski berbeda beda setiap platform, namun aturan awal dari setiap program sukarela ini biasanya mencakup kerahasiaan, etika, dan keamanan sistem itu sendiri.

5. **Dalam melakukan kolaborasi pemerintah dan masyarakat, Bagaimana Anda sebagai praktisi keamanan siber memandang pentingnya hubungan saling ketergantungan antara seluruh pihak yang terlibat dalam program ini?**

   Jawab:

   Menurut hemat saya, dengan banyaknya sistem digital yang dibuat oleh pemerintah serta banyaknya kebocoran data, timbul urgensi dari pemerintah untuk mengamankan sistem elektronik yang dibuat, hal ini tentunya tidak akan dapat dipenuhi oleh BSSN sendirian. Masyarakat dan praktisi dengan segudang prestasi di lomba keamanan siber pun mulai bermunculan dari Indonesia, potensi ini tentu akan menjadi sia-sia dan tidak akan berkembang apabila pemerintah tidak memberikan sebuah wadah yang proporsional. Oleh karena itu, muncullah sebuah hubungan saling ketergantungan antara PSE dengan BSSN, BSSN dengan masyarakat dan praktisi keamanan siber, serta PSE dengan masyarakat dan praktisi keamanan siber.

6. **Apakah Anda memberikan investasi awal untuk mengikuti program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Seperti biaya pendaftaran, atau investasi dalam bentuk lain. Berkenan anda dapat menjelaskan secara lengkap.**

   Jawab:

   Investasi yang saya lakukan ialah dengan membeli VPS sendiri serta lisensi *tools*, seperti burpsuite dan IDAPro.Untuk menjamin terselenggaranya program Identifikasi kerentanan dan Proteksi Secara Sukarela dibutuhkan komitmen bersama antar seluruh entitias yang terlibat, baik dari penyelenggara, pemilik sistem elektronik, dan para praktisi keamanan siber.

7. **Apakah Anda memiliki komitmen terhadap proses kolaboratif dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawab:

   Ya, saya memiliki komitmen penuh untuk ikut berkolaborasi dalam program ini, hal ini karena saya telah berkomitmen untuk melakukan pengamanan siber bagi pemerintah secara sukarela dan memenuhi portofolio saya dengan hal tersebut.

8. **Bagaimana Anda selaku praktisi keamanan siber dapat membangun kepercayaan dengan seluruh aktor yang terlibat dalam program ini? Adakah klausul / prasyarat yang dapat dijadikan acuan?**

   Jawab:

   Saya bersedia untuk mengisi NDA dan nota kesepahaman lainnya dengan data pribadi saya yang dijamin keasliannya. Setelah *report* saya kirimkan saya juga hanya akan mempublikasikan *report* tersebut apabila mendapat persetujuan pemilik sistem, tentunya dengan menutupi path atau parameter aslinya.

9. **Berdasarkan pengalaman Anda, apakah anda pernah bekerjasama dengan instansi pemerintah? Jika pernah, bagaimana anda menjaga hubungan tersebut jika dikaitkan dengan program yang ditetapkan oleh BSSN untuk mendukung keberlangsungan proses kolaborasi?**

   Jawab:

   Saya pernah menjalani kerjasama dengan salah satu Diskominfo di pulau Jawa dalam pelaksanaan magang saya. Magang pertama saya diminta untuk melakukan verifikasi hasil *vulnerablity scanning* yang merupakan agenda rutin dari Diskominfo tersebut terhadap aplikasi di daerahnya. Dalam menjaga hubungan tersebut saya berusaha memberikan yang terbaik pada saat pelaksanaan dan ikut bergabung dengan komunitas yang telah disediakan oleh Diskominfo tersebut guna tetap berkontribusi apabila terdapat sistem baru yang dibuat.

10. **Dalam melaksanakan identifikasi kerentanan dan/atau memberikan rekomendasi proteksi dibutuhkan ruang lingkup yang jelas dan tepat. Apakah anda selaku praktisi keamanan siber dapat memutuskan bahwa anda sepakat dengan ruang lingkup pekerjaan dalam program yang diselenggarakan?**

    Jawab:

    Ya, Kami dapat memutuskan sepakat atau tidaknya dengan ruang lingkup pekerjaan yang diberikan, dan kami dapat mencari program lain apabila program tersebut tidak sesuai dengan ruang lingkup pekerjaan kami.

11. **Ketika anda mengikuti program Identifikasi kerentanan dan proteksi secara sukarela, tentunya mendapatkan berbagai informasi sensitif terkait kerentanan dan sistem elektronik terkait, dan memungkinkan mendapatkan informasi sensitif lainnya seperti data pribadi. Bagaimana Anda selaku praktisi keamanan siber mengelola pengetahuan yang didapat selama proses kolaborasi?**

    Jawab:

Seluruh data yang telah terekstrak pada saat proses pengujian tidak akan diperjualbelikan dan langsung dihapus ketika telah terdapat informasi bahwanya pengamanan telah dilakukan.

12. **Dari program yang anda ikuti, apakah penyelenggara dan/atau pemilik sistem elektronik memberikan hak-hak apresiasi berdasarkan kontribusi anda ?**

    Jawab:

    Ya, mereka memberi hak apresiasi terhadap Saya berdasarakan tingkat dampak yang telah saya temukan.

13. **Jika dalam pelaksanaannya, Anda berhasil menemukan kerentanan lain terkait ruang lingkup pengujian pada media online sumber terbuka (*open source*) baik berupa dugaan kebocoran data, atau informasi sensitif lainnya. Apakah anda bersedia untuk melaporkan ke penyelenggara program dan/atau pemilik sistem elektronik sebagai bentuk komitmen anda untuk menjadi Hacker Baik?**

    Jawab:

    Ya, Saya akan melaporkannya agar tidak ada percobaan masuk setelah data bocor menggunakan kredensial untuk masuk mengalami kebocoran

14. **Bagaimana Anda menilai program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil?**

    Jawab: :

    Program Identifikasi Kerentanan dan Proteksi secara sukarela berhasil ketika kolaborasi tetap berjalan hingga berkembang dengan mekanisme yang lebih efektif dan hadiah hadiah yang lebih menarik ke depannya sehingga animo masyarakat tidak akan berkurang

Lampiran 6 Transkrip Wawancara 5

PSE Lingkup Publik

Narasumber : Ryandi Yusuf

Peran : PSE Lingkup Publik – Kejaksaan Agung

Tanggal : 30 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Dengan adanya program kolaborasi yang ditetapkan BSSN, apakah organisasi anda selaku PSE Lingkup publik memungkinkan berpartisipasi dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawaban:

   Memungkinkan

2. **Menurut pandangan Anda, hal apa yang mendasari tujuan kolaborasi melalui program ini jika dikaitkan dengan implementasi keamanan siber di organisasi anda?**

   Jawaban:

   Tujuan kolaborasi pada program ini sejalan dengan tujuan dari keamanan siber pada organisasi kami, yaitu dalam penegakan hukum. Tujuan organisasi kami tentunya dalam rangka menghadirkan kepastian hukum serta melindungi kepentingan umum di bidang penegakan hukum. Sehingga jika terjadi suatu serangan siber yang dapat mengganggu kinerja organisasi kami, tentunya tujuan awal akan mengalami hambatan serta berdampak terhadap penurunan kepercayaan masyarakat terhadap organisasi kami.

3. **Menurut pandangan Anda, bagaimana Organisasi Anda akan memberikan respon terhadap rencana BSSN dalam menyelenggarakan program Identifikasi Kerentanan dan Proteksi Secara Sukarela ini?**

   Jawaban:

   Organisasi kami tentunya akan menjalin koordinasi dan partisipasi aktif serta keikutsertaan dalam membangun dan mendukung program ini dengan BSSN

sebagai pusatnya. Kami meyakini bahwa keberhasilan program ini bukan hanya berada di pihak BSSN saja, tetapi seluruh pengguna, termasuk organisasi kami yang terlibat di dalamnya.

4. **Berdasarkan kondisi yang ada, apakah organisasi anda telah memiliki aturan awal (*preliminary rules*) yang dijadikan acuan dalam dalam penyelenggaraan program serupa (jika ada), baik dalam hal identifikasi kerentanan maupun pemberian rekomendasi pengamanan?**

   Jawaban:

   Saat ini acuan penyelenggaraan program di organisasi kami belum dituangkan ke dalam peraturan, dan masih dalam proses pengusulan, sehingga segala bentuk acuan masih berpegangan pada aturan di BSSN.

5. **Bagaimana organisasi Anda menyikapi proses kolaborasi ini? Apakah terlihat adanya potensi saling membutuhkan diantara seluruh pihak yang terlibat dalam kolaborasi? Baik dari BSSN, para pegiat keamanan siber, maupun Organisasi Anda?**

   Jawaban:

   Organisasi kami menilai bahwa keterlibatan seluruh elemen di dalam program ini menjadi kunci keberhasilan dari program kolaborasi ini. Di internal organisasi, peran pelaksana hingga pimpinan menjadi penting dalam menjalankan program kolaborasi, sedangkan di eksternal organisasi, komunikasi dan koordinasi menjadi jembatan yang penting untuk menciptakan suatu ikatan keterkaitan antara bssn selaku organisasi induk dengan organisasi kami sebagai pengguna.

6. **Selain dukungan kebijakan, apakah organisasi Anda memandang bahwa dukungan dalam bentuk investasi jenis lain yang dapat diberikan sebagai bentuk apresiasi kepada praktisi keamanan siber untuk mendukung keberhasilan program tersebut? Jika iya terdapat investasi jenis lain, maka jenis investasi apa yang akan diberikan?**

   Jawaban:

Organisasi kami memandang bahwa kebijakan memberikan suatu kepastian terhadap keberlangsungan program tersebut, sedangkan dukungan anggaran (operasional, reward/penghargaan, dan dukungan lain) merupakan bentuk nyata terhadap dukungan dan keseriusan terhadap program tersebut. Adapun investasi lainnya pada program tersebut berbentuk kolaborasi dan penunjukan sebagai narasumber maupun sebagai konsultan, sehingga memberikan dukungan dalam bentuk nyata yang diakui oleh negara dalam hal pertanggungjawaban anggaran.

7. **Jika organisasi Anda berminat mengikuti program identifikasi dan kerentanan secara sukarela (VVIP BSSN), bagaimana komitmen organisasi anda terhadap proses kolaboratif melalui program ini?**

   Jawaban:

   Komitmen organisasi kami dalam mengikuti program VVIP tersebut tentunya berawal dari koordinasi dan komunikasi aktif dengan BSSN dalam pembentukan pondasi awal pada program tersebut, sehingga hal-hal yang menjadi dasar program tersebut tidak terlewatkan.

8. **Selanjutnya dari pengalaman Anda, Bagaimana organisasi anda dapat membangun kepercayaan dengan seluruh pihak yang terlibat dalam program ini? baik dari BSSN maupun dengan para pegiat keamanan siber?**

   Jawaban:

   Dengan komunikasi aktif, baik secara langsung maupun tidak langsung, serta penyampaian informasi di saluran resmi organisasi dengan memberikan suatu pemberitaan dan penyampaian reward dalam bentuk investasi lainnya sehingga dapat menggugah keikutsertaan dari pihak eksternal dalam mensukseskan program tersebut.

9. **Berdasarkan pengalaman, bagaimana organisasi Anda menjaga hubungan internal dan eksternal untuk mendukung keberlangsungan proses kolaborasi?**

   Jawaban:

   Di internal, pengalaman organisasi kami di level pimpinan memang mengalami kendala, karena tupoksi mengenai kemanan siber belum menjadi perhatian pimpinan organisasi, baik di level daerah maupun di level pusat, sehingga pengajuan program, baik dari kebijakan hingga dukungan anggaran mengalami keterlambatan dalam penyelesaiannya. Namun dari level pelaksana, pemahaman mengenai program VVIP menjadi topik utama yang menjadi bagian penting terhadap perlindungan keamanan siber yang ada di organisasi, sehingga jalan keluar dari permasalahan tersebut adalah adanya komunikasi yang efektif yang disampaikan kepada pimpinan organisasi.

   Di eksternal, pengalaman organisasi kami sebenarnya belum bersinggungan dengan pihak di luar pemerintahan. Sehingga yang terjadi saat ini adalah keterikatan dengan BSSN selaku organisasi pemerintah yang membidangi permasalahan keamanan informasi dan keamanan siber.

10. **Pada saat mendaftarkan diri untuk mengikuti program identifikasi kerentanan dan proteksi secara sukarela, Bagaimana organisasi Anda menetapkan ruang lingkup yang dikerjakan telah sesuai dengan harapan Anda? Apakah terdapat koordinasi antar seluruh pihak yang terlibat dalam program kolaborasi?**

    Jawaban:

    Organisasi kami menetapkan fungsi dan kewenangan pihak-pihak yang terlibat di dalam program VVIP tersebut, selanjutnya menetapkan jalur koordinasi sehingga komunikasi dapat berjalan secara efektif ketika program telah dijalankan.

11. **Menurut pandangan Anda, bagaimana langkah organisasi Anda dalam mengelola pengetahuan yang didapat dari proses kolaborasi?**

    Jawaban:

Organisasi kami menilai saat ini, pengetahuan mengenai tujuan program VVIP ini masih terbatas di satuan kerja yang membidangi keamanan informasi dan keamanan siber yang ada di Organisasi kami, sehingga belum seluruh satuan kerja yang ada di organisasi kami memahami dengan baik tujuan dan manfaat dari program VVIP tersebut. Oleh sebab itu, masih banyaknya tugas dan pekerjaan rumah (PR) yang harus dilakukan oleh Organisasi kami agar pengetahuan dan informasi tersebut dapat diterima di seluruh satuan kerja.

12. **Menurut pandangan Anda, apakah seluruh pihak telah menerima manfaat berdasarkan investasi yang telah dilakukan dalam program identifikasi dan kerentanan secara sukarela ini?**
    Jawaban:
    Belum seluruhnya

13. **Menurut pandangan Anda, apakah dalam penyeleggaraan program ini telah menerapkan asas transparansi dan akuntabilitas?**
    Jawaban:
    Belum dapat menilai bahwa asas transparansi dan akuntabilitas telah hadir dalam penyelenggaraan program VVIP tersebut dikarenakan belum berjalannya program VVIP tersebut di organisasi kami.

14. **Menurut pengalaman Anda, bagaimana organisasi Anda menilai program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil?**
    Jawaban:
    Organisasi kami menilai bahwa program VVIP tersebut dapat dikatakan berhasil jika seluruh dukungan dari pihak-pihak yang terlibat, baik internal maupun eksternal dapat berjalan sesuai dengan fungsinya, ditambah dengan adanya koordinasi aktif sehingga seluruh pihak dapat terlibat dan merasa memiliki program VVIP tersebut.

Lampiran 7
Transkrip Wawancara 6

Pegiat Keamanan Siber

Narasumber : Subroto Budhi Utomo
Peran : PSE Lingkup Publik – Jawa Tengah
Tanggal : 28 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Dengan adanya program kolaborasi yang ditetapkan BSSN seperti VVIP Program, apakah organisasi anda selaku PSE Lingkup publik memungkinkan berpartisipasi dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela ?**

   Jawaban

   Sangat mungkin sekali kami akan berpartisipasi dalam program tersebut.

2. **Menurut pandangan Anda, hal apa yang mendasari tujuan kolaborasi melalui program ini jika dikaitkan dengan implementasi keamanan siber di organisasi anda?**

   Jawaban

   Program kolaborasi ini akan sangat membantu meningkatkan keamanan sistem elektronik dan aplikasi milik Pemerintah Provinsi Jawa Tengah. Karena dengan adanya program ini dapat di deteksi kemungkinan ada kerentanan keamanan yang tidak terdeteksi oleh tim internal. Selain itu program ini diharapkan dapat meningkatkan respon terhadap ancaman siber yang semakin meningkat.

3. **Menurut pandangan Anda, bagaimana Organisasi Anda akan memberikan respon terhadap rencana BSSN dalam menyelenggarakan program Identifikasi Kerentanan dan Proteksi Secara Sukarela ini ?**

   Jawaban

   Pemerintah Provinsi Jawa Tengah sangat merespon secara positif dengan adanya program ini, dikarenakan manfaat dari program ini yang dapat membantu dalam mendeteksi adanya kerentanan pada sistem serta bagaimana melakukan mitigasinya.

4. **Berdasarkan kondisi yang ada, apakah organisasi anda telah memiliki aturan awal (preliminary rules) yang dijadikan acuan dalam dalam penyelenggaraan program serupa (jika ada), baik dalam hal identifikasi kerentanan maupun pemberian rekomendasi pengamanan yang bekerjasama dengan pihak eksternal organisasi?**

   Jawaban

   Secara tertulis, Pemerintah Provinsi Jawa Tengah belum memiliki preliminary rules dalam penyelenggaraan serupa, namun kami telah menerapkan aturan-aturan yang tidak tertulis / best practise dalam menerima pengaduan/pelaporan mengenai temuan celah keamanan pada sistem/aplikasi dari masyarakat.

5. **Bagaimana organisasi Anda menyikapi proses kolaborasi ini? Apakah terlihat adanya potensi saling membutuhkan diantara seluruh pihak yang terlibat dalam kolaborasi? Baik dari BSSN, para pegiat keamanan siber, maupun Organisasi Anda?**

   Jawaban

   Dengan adanya kolaborasi ini maka diharapkan semua pihak dapat memperoleh keuntungan / mutualisme seperti pihak PSE dapat mengetahui adanya celah keamanan pada sistem, penggiat keamanan siber dapat menyalurkan bakatnya secara legal tanpa harus khawatir adanya konsekuensi hukum serta mendapatkan reward baik berupa material maupun immaterial, selain itu BSSN juga dapat memonitor dan mengarahkan penggiat siber untuk tujuan yang baik dan meminimalisir terjadinya insiden siber yang dikarenakan adanya penggiat keamanan siber yang melakukan serangan terhadap sistem/aplikasi yang sudah berjalan.

6. **Selain dukungan kebijakan, apakah organisasi Anda memandang bahwa dukungan dalam bentuk investasi jenis lain yang dapat diberikan sebagai bentuk apresiasi kepada praktisi keamanan siber untuk mendukung keberhasilan program tersebut?**

   Jika iya terdapat investasi jenis lain, maka jenis investasi apa yang akan diberikan?

   Jawaban

Organisasi dapat mengalokasikan dana untuk menjadikan praktisi keamanan siber sebagai narasumber ataupun pelatih bagi tim keamanan siber organisasi agar dapat terus meningkatkan keterampilan dan pengetahuan mereka. Selain itu, Organisasi dapat menyediakan kesempatan bagi para bug hunter untuk berkolaborasi dengan tim keamanan siber organisasi dalam proyek-proyek penelitian keamanan atau pengembangan alat keamanan baru. Hal ini tidak hanya memberikan manfaat bagi organisasi dalam meningkatkan keamanan mereka, tetapi juga memberikan kesempatan bagi para bug hunter untuk memperluas jaringan mereka dan mendapatkan pengalaman yang berharga.

7. **Jika organisasi Anda berminat mengikuti program identifikasi dan kerentanan secara sukarela (VVIP BSSN), bagaimana komitmen organisasi anda terhadap proses kolaboratif melalui program ini?**

   Jawaban

   Kami akan segera menindak lanjuti temuan kerentanan pada sistem elektronik milik Pemerintah Provinsi Jawa Tengah dengan melakukan perbaikan dan penutupan celah keamanan sesuai rekomendasi.

8. **Selanjutnya dari pengalaman Anda, Bagaimana organisasi anda dapat membangun kepercayaan dengan seluruh pihak yang terlibat dalam program ini? baik dari BSSN maupun dengan para pegiat keamanan siber?**

   Jawaban

   - Menerapkan Non Disclosure Agreement dalam setiap kegiatan, Organisasi harus memastikan bahwa mereka mematuhi semua regulasi dan standar keamanan yang relevan. Ini termasuk regulasi terkait perlindungan data pribadi, standar keamanan jaringan, dan persyaratan pelaporan insiden keamanan.
   - Penyelenggara harus Memberikan Pengakuan dan Apresiasi, berupa pengakuan dan menghargai kontribusi yang diberikan oleh para praktisi keamanan siber dalam meningkatkan keamanan organisasi. Ini dapat dilakukan melalui penghargaan resmi, pengakuan publik, atau kesempatan untuk berkolaborasi secara lebih dalam dalam program keamanan siber.

9. **Berdasarkan pengalaman, bagaimana organisasi Anda menjaga hubungan internal dan eksternal untuk mendukung keberlangsungan proses kolaborasi?**

   Jawaban

   Untuk menjaga hubungan dalam mendukung keberlangsungan kolaborasi dibentuklah sebuah grup/perkumpulan serta sering dilakukan tukar pikiran dalam membahas sebuah kasus yang hangat, selain itu melakukan pertemuan rutin dan berbagi informasi juga dapat meningkatkan kolaborasi.

10. **Pada saat mendaftarkan diri untuk mengikuti program identifikasi kerentanan dan proteksi secara sukarela, Bagaimana organisasi Anda menetapkan ruang lingkup yang dikerjakan telah sesuai dengan harapan Anda? Apakah terdapat koordinasi antar seluruh pihak yang terlibat dalam program kolaborasi?**

    Jawaban

    Sebelum pelaksanaan program dilakukan koordinasi terlebih dahulu dengan pemilik Sistem Elektronik yang akan dijadikan target untuk mengetahui cara kerja, mempersiapkan data dummy serta kredensial pengujian, selain itu dilakukan duplikasi terhadap sistem dan ditempatkan pada lingkungan khusus pengujian. Hal ini perlu dilakukan agar pengujian dapat berlangsung secara maksimal dan tidak keluar dari ruang lingkup pengujian yang sudah ditetapkan.

11. **Menurut pandangan Anda, bagaimana langkah organisasi Anda dalam mengelola pengetahuan yang didapat dari proses kolaborasi?**

    Jawaban

    Dilakukan PoC ulang terhadap temuan yang diberikan oleh para peserta, selain itu kami melakukan dokumentasi terhadap PoC yang telah kami dapatkan, sehingga dapat dijadikan sebagai ilmu pembelajaran bagi kami.

12. **Menurut pandangan Anda, apakah seluruh pihak telah menerima manfaat berdasarkan investasi yang telah dilakukan dalam program identifikasi dan kerentanan secara sukarela ini?**

    Jawaban

    Seluruh pihak telah menerima manfaat program ini, pihak PSE dapat mengetahui adanya celah keamanan pada sistem, penggiat keamanan siber

dapat menyalurkan bakatnya secara legal tanpa harus khawatir adanya konsekuensi hukum serta mendapatkan reward baik berupa material maupun immaterial, selain itu BSSN juga dapat memonitor dan mengarahkan penggiat siber untuk tujuan yang baik dan meminimalisir terjadinya insiden siber yang dikarenakan adanya penggiat keamanan siber yang melakukan serangan terhadap sistem/aplikasi yang sudah berjalan.

13. **Menurut pandangan Anda, apakah dalam penyelenggaraan program ini telah menerapkan asas transparansi dan akuntabilitas?**

    Jawaban

    Dalam pelaksanaan program ini telah diterapkan asas transparansi, kami selaku PSE telah diberikan kredensial akun aplikasi website BSSN VVIP program untuk melihat dan mengamati hasil dan keberlangsungan program.

14. **Menurut pengalaman Anda, bagaimana organisasi Anda menilai program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil?**

    Jawaban

    Program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil apabila seluruh pihak dalam memahami perannya dalam program ini. Bagi kami selaku PSE, kami segera melakukan tindak lanjut perbaikan terhadap temuan kerentanan tersebut.

Lampiran 1
Pedoman Wawancara

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 TAHUN 2023

Tujuan Wawancara:

Wawancara dilakukan untuk mengetahui 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 (SPBE). Selain itu untuk mengetahui kolaborasi pemerintah dan masyarakat dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela, peneliti juga ingin mendapatkan informasi mengenai faktor-faktor yang mempengaruhi dalam proses kolobaorasi tersebut. Dengan demikian diharapkan dapat tergambarkan mekanisme dan faktor yang mendukung maupun menghambat dalam kolaborasi pemerintah dan masyarakat melalui program Identifikasi Kerentanan dan Proteksi Secara Sukarela yang ditetapkan oleh BSSN.

Informan Penelitian:

Informan terbagi menjadi pegawai dengan jabatan struktural dan pegawai fungsional atau jabatan non struktural di lingkungan Direktorat Operasi Keamanan Siber, BSSN, PSE Lingkup Publik dan Pegiat keamanan siber selaku perwakilan dari masyarakat.

Kisi – Kisi Pedoman Wawancara:

Dimensi	Sub Dimensi	Indikator
Antecendents	*Multiple Actors*	Keterlibatan banyak aktor akan memberikan informasi dan sumber daya yang heterogen
	Common goals	Terdapat kesadaran, dan tujuan yang sama dalam melaksanakan kolaborasi
	Facilitative leadership	Adanya salah satu pihak yang bertindak sebagai leader untuk menginisiasi program
	Preliminary rules	Adanya aturan yang dijadikan acuan dalam penyelenggaraan program sesuai dengan perannya masing-masing
	Interdependece perception	Program hanya dapat terselenggara apanila pihak penyelenggara, pemilik sistem, dan masyarakat selaku pengidentifikasi kerentanan dan/atau pemberi rekomendasi telah tersedia dan sepakat untuk menjalankan program ini
	Initial invesment	Adanya investasi awal dari penyelenggara untuk memulai proses kolaboratif, seperti dasar hukum, tata kelola, petunjuk teknis, aturan, sumber daya keuangan, manusia, teknologi, dan dukungan lainnya, serta aset *intangible* seperti pengetahuan, status, identitas, ideologi, budaya, dan keterampilan yang mendukung penyelenggaraan program.
Collaborative Process	*Commitmen to the process*	Terdapat komitmen antara seluruh aktor yang terlibat, baik penyelenggara, pemilik sistem elektronik, maupun masyarakat selaku pengidentifkasi dan/atau pemberi rekomendasi keamanan siber.
	Trust building	Membangun kepercayaan antar seluruh aktor yang terlibat
	Internal and external relationship	Adanya komunikasi yang intens baik secara internal, dan/atau eksternal organisasi untuk menciptakan keberlangsungan proses kolaborasi
	Consensus building	Ruang lingkup pekerjaan sesuai dengan apa yang disepakati sejak awal penyelenggaraan program
	Knowledge management	Adanya pengaturan pengetahuan yang telah didapat dan dibagikan kembali ke seluruh pihak yang terlibat

Dimensi	Sub Dimensi	Indikator
Equity Outcomes	*Multiple investment sources*	Adanya investasi dari berbagai pihak yang mendukung penyelenggaraan program, seperti kontribusi pemberian apresiasi terhadap masyrakat yang menjadi pengidentifikasi dan/atau pemberi rekomendasi keamanan.
	Accountability	Adanya transparansi dalam penyelenggaraan program yang dilakukan oleh entitas yang terlibat sebagai bentuk pertanggungjawaban
	Discoure and practice	Adanya hasil yang sesuai dengan tujuan awal kolaborasi, yakti hasil identifikasi kerentanan dan/atau rekomendasi pengamanan

Lampiran 2
Transkrip Wawancara 1

Ketua Tim ITSA Direktorat Operasi Keamanan Siber

Narasumber : Taufik Nurhidayat, S.ST
Jabatan : Ketua Tim IT *Security Assessment*, Direktorat Operasi Keamanan Siber
Unit Kerja : Direktorat Operasi Keamanan Siber, Deputi II BSSN
Tanggal : 5 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Bagaimana Tim ITSA dalam melibatkan Personilnya pada program Identifikasi Kerentanan dan Proteksi Secara Sukarela, terutama dalam konteks identifikasi kerentanan aplikasi SPBE? Apakah dengan keterlibatan tersebut akan memperkaya pandangan dan pengetahuan, sehingga dapat menjadi solusi atas keamanan siber di sektor pemerintahan?**

   Jawaban:

   Keterlibatan Tim dalam penyelenggaraan program Identifikasi Kerentanan dan Proteksi secara Sukarela ini memang didasari oleh komitmen bersama antara staf bersama pimpinan di BSSN. Hal ini dipengaruhi juga adanya sejumlah kondisi seperti munculnya banyak permintaan layanan ITSA dari stakeholder, keterbatasan sumber daya yang dimiliki BSSN untuk mengakomodir seluruh permintaan, serta adanya potensi pelibatan sumber daya di luar BSSN dari kalangan komunitas, Pegiat keamanan siber dan pihak lainnya untuk dapat terlibat dalam kegiatan identifikasi kerenanan. Selanjutnya secara spesifik program identifikasi kerentanan dan proteksi secara sukarela masih selaras dengan visi-misi BSSN terutama dalam hal menumbuh kembangkan talenta keamanan siber di luar BSSN.

   Adapun upaya yang telah dilakukan oleh Tim ITSA BSSN secara bersama-sama dengan pihak-pihak terkait di BSSN antara lain:

a. Penyiapan Sumber Daya Manusia

Secara Internal SDM di Tim ITSA telah mempersiapkan kemampuan di bidang identifikasi kerentanan guna mendukung pelaksanaan program Identifikasi Kerentanan dan proteksi secara sukarela. Adapun peran Tim ITSA yang menguasa Identifikasi kerentanan dapat membantu dalam sebagai verifikator terhadap laporan identifikasi kerentanan yang masuk pada saat program berjalan. Hal ini sebagaimana tertuang dalam Peraturan Kepala BSSN tentang program ini, BSSN menempatkan diri sebagai koordinator, sehingga tidak dapat terlibat langsung dalam proses identifikasi.

Dengan melihat potensi kedepan sangat besar, Tim ITSA juga telah berkolaborasi dengan pihak-pihak di luar Tim, sehingga kita juga sudah dapat menambah SDM, dan sangat memungkinkan untuk dilaksanakan dan ini juga telah dikomunikasikan kepada pimpinan. Dan juga melihat juga cakupan pekerjaan, sehingga resource perlu disesuaikan.

Secara Eksternal, Tim ITSA bersama tim lain di BSSN juga telah komunitas / Pegiat keamanan sinber, dengan melakukan pendekatan kepada komunitas secara format / informal (kedekatan), secara formal melakukan pendekatan secaui unit kerja pembinaan SDM Siber (D41). Pendekatan tersebut masih kita *maintenance*, baik kegiatan bersama temen2 komunitas, baik kegiatan werbinar, seminar, dabhak kegiatan IK. Untuk menjaga hubungan, kita jg sudah membuat grup chat telegram, sbg upaya akomodir mereka.

b. Penyiapan Proses / Tata Kelola

Dalam menjalankan kolaborasi penting untuk memperhatikan aturan yang dijadikan pedoman. Oleh karena itu, Tim ITSA terlibat juga dalam penyusunan Peraturan Kepala tentang pelaksanaan program IK dan Prokteksi ini, adapun semua ketentuan yang nantinya digunakan sebagai acuan sudah masuk ke masuk ke Perka tersebut. Dengan demikian diharapkan dapat membantu dalam penyelenggaraan program IK dan Prokteksi. Apabila dalam pelaksanaan membutuhkan hal-hal yang lebih detail, kami bersama Tim Program juga telah menyusun juknis, SOP, dan semua instrumen tersebut juga perlu disimulasikan mulai aturan main, dan

bagaimana peran dari masing-masing pihak yang terlibat. Jangan sampai ada hal-hal yang terlewat, dan mengganggua jalannya kegiatan. Baik dari prosedur yang dilewatkan, ataupun administrasi kegiatan seperti penandatangan perjanjian kerjasama seperti NDA, danan harapanya tidak ada pihak yang melanggar hukum.

c. Penyiapan Teknologi

Tim ITSA bersama tim penyusun program juga telah mengembangkan platform Identifikasi Kerentanan dan Proteksi yang dapat digunakan oleh seluruh pihak mulai dari BSSN, PSE Lingkup Publik, maupun Pegiat keamanan siber seperti Bug hunter. Namun dalam penyelenggaraan ini akan lebih baik jika ke depannya dapat dimanfaatkan oleh entitas lain yang bertugas sebagai tim pengawas.

2. Apa tujuan bersama yang ingin dicapai oleh Tim ITSA melalui program ini, khususnya dalam meningkatkan keamanan aplikasi SPBE melalui kegiatan identifikasi kerentanan?

Jawaban:

Berangkat dari tugas pokok dan fungsi BSSN, yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber. Dalam meningkatkan keamanan SPBE, BSSN perlu mengkolaborasikan seluruh stakeholder di Indonesia tidak hanya entitas pemerintah, industri, akademisi. Namun juga entitas komunitasi perlu dirangkul dalam rangka kolaborasi.

Sejalan dengan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Isber Nasional dan Manajemen Krisis Siber. BSSN dapat bergerak dan berkolaborasi dalam Quadhelix stakeholder. Quad Helix yang dimaksud meliputi unsur pemerintah, pelaku bisnis, akademisi, seta masyarakat atau komunitas. Keempat pemangku kepentingan tersebut dilibatkan sebagai upaya mendukung strategi keamanan siber nasional.

Kemudiaan setiap pemerintah, dalam menjalankan tugasnya tentunya akan menilai dan mengukur, berapa *outcome* yang berkaitan langsung tentang kesejahteraan yang dirasakan oleh masyarakat. Khusus untuk masyarakat

keamanan siber, melalui Program IK dan Proteksi ini diharapkan bisa dijadikan tempat mencari pengalaman, protofolio sabagai modal awal dalam terjun di bidang industri keamanan siber. Mereka bisa menerima, manfaatkan, dan mendapatkan pekerjaan sehingga dapat meningkat kesejahteraan mereka.

Keamanan siber juga disampaikan para ahli, Indonesia membutuhkan komponen cadangan. Komunitas kamsiber, sbg bentuk komcad, sehingga perlu dibina oleh BSSN. Jangan samapai digunakan untuk kriminilas, atau hal yang merugikan. Kita juga bisa menggali aspirasi dari kominitas, ini seperti apa. Terkait kamsiber yang diselenggarakan oleh BSSN, atau yang mengakomodir untuk mereka berkembang

3. **Adakah aturan awal yang dijelaskan kepada tim ITSA sebagai acuan dalam penyelenggaraan program Identifikasi Kerentanan dan Proteksi Secara Sukarela di konteks identifikasi kerentanan?**

   Jawaban:

   Dalam menjalankan kolaborasi penting untuk memperhatikan aturan yang dijadikan pedoman. Oleh karena itu, Tim ITSA terlibat juga dalam penyusunan Peraturan Kepala tentang pelaksanaan program IK dan Prokteksi ini, adapun semua ketentuan yang nantinya digunakan sebagai acuan sudah masuk ke masuk ke Perka tersebut. Dengan demikian diharapkan dapat membantu dalam penyelenggaraan program IK dan Prokteksi.

   Apabila dalam pelaksanaan membutuhkan hal-hal yang lebih detail, kami bersama Tim Program juga telah menyusun juknis, SOP, dan semua instrumen tersebut juga perlu disimulasikan mulai aturan main, dan bagaimana peran dari masing-masing pihak yang terlibat. Jangan sampai ada hal-hal yang terlewat, dan mengganggua jalannya kegiatan. Baik dari prosedur yang dilewatkan, ataupun administrasi kegiatan seperti penandatangan perjanjian kerjasama seperti NDA, dan harapanya tidak ada pihak yang melanggar hukum.

4. **Sebagai Ketua Tim ITSA, bagaimana Anda mendukung dan memfasilitasi anggota tim dalam menjalankan program ini, dengan tidak meninggalkan tugas dan fungsi Tim ITSA sehari-hari?**

Jawaban:

Secara Internal SDM di Tim ITSA telah mempersiapkan kemampuan di bidang identifikasi kerentanan guna mendukung pelaksanaan program Identifikasi Kerentanan dan proteksi secara sukarela. Adapun peran Tim ITSA yang menguasa Identifikasi kerentanan dapat membantu dalam sebagai verifikator terhadap laporan identifikasi kerentanan yang masuk pada saat program berjalan. Hal ini sebagaimana tertuang dalam Peraturan Kepala BSSN tentang program ini, BSSN menempatkan diri sebagai koordinator, sehingga tidak dapat terlibat langsung dalam proses identifikasi.

Dengan melihat potensi kedepan sangat besar, Tim ITSA juga telah berkolaborasi dengan pihak-pihak di luar Tim, sehingga kita juga sudah dapat menambah SDM, dan sangat memungkinkan untuk dilaksanakan dan ini juga telah dikomunikasikan kepada pimpinan. Dan juga melihat juga cakupan pekerjaan, sehingga resource perlu disesuaikan.

5. **Bagaimana persepsi interdependensi antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber dalam menjalankan program ini? Bagaimana Anda melihat peran tim ITSA dalam mencapai tujuan kolaboratif, terutama dalam konteks identifikasi kerentanan?**

   Jawaban:

   Persepsi interdependensi antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber menunjukkan hubungan ketergantunganm dimana terdapat adanya kebutuhan IK dari PSE, atas kebutuhan mereka. Di sisi lain mereka tidak punya resource, sehingga munculnya entitas baru (komunitas) sebagai peluang untuk membantu PSE dalam melakukan identifikasi kerentanan melalui program ini.

   Selanjutnya bagaimana, adanya hubungan keterkaitam, timbal balik dari masing-masing pihak, diantaranya seperti:

   a. PSE Lingkup Publik akan mendapatkan layanan IK dan proteksi akibat kurang resource dari PSE itu sendiri.
   b. Bug hunter juga membutuhkan portofolio sebagai modal mencari pekerjaan atau kegiatan lain seperti peningkatan kapabilitas, sertifikasi keahlian di bidang keamanan siber. Selain itu adanya rasa prestis / pernghargaan yang

akui dan diterbitkan oleh BSSN yang harapannya akan meningkatkan nilai pada saat mencari pekerjaan. Dimana BSSN merupakan lembaga pemerintah yang bergerak dan membina bidang keamanan siber di Indonesia.

c. BSSN juga menjadi pihak yang membutuhkan pihak lainnya dalam meningkatkan ekosistem keamanan siber di Indonesia. BSSN menajdi pihak yang dapat menghubungkan antara PSE Lingkup Publik dan masyarakat. Dimana ketika bug hunter atau Pegiat keamanan siber melakukan komunikasi / hubunan langsung dengan PSE Lingkup Publik, belum sepenuhnya saling percaya bahkana bisa jadi tidak percaya. Sehingga kehadiran BSSN menjadi perantara yang baik bagi kedua belah pihak.

6. **Bagaimana Tim ITSA membangun dan mempertahankan kepercayaan dalam tim internal dan kolaborasi eksternal khususnya hubungan antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber dalam konteks identifikasi kerentanan?**

   Jawaban:

   Untuk membangun kepercayaan dalam konteks Identifikasi kerentanan, secara internal Tim ITSA telah memiliki pemahaman yang akan tupoksi dan tanggunjawab masing-masing personil di Tim ITSA. Dengan berbekal kemampuan yang dimiliki oleh personil Tim ITSA yang mana secara keseluruhan adalah Lulusan dari Sekolah Tinggi Sandi Negara atau Politeknik Siber dan Sandi Negara. Sehingga tim telah dibekali dengan kemampuan yang cukup, sehingga kami percaya akan seluruh tim yang ada, dan dapat menjalankan tugas dan tanggung jawab sesuai kebutuhan organisasi.

   Selanjutnya secara ekternal dengan pihak-pihak lain seperti PSE Lingkup Publik, dan Pegiat Keamanan Siber, Tim juga telah menjaga hubungan yang baik dengan PSE Lingkup Publik telah menjalin hubungan kerjasama di bidang identifikasi melalui layanan IT *Security Assessment*. Kemudian juga telah menjalin hubungan dengan Pegiat Keamanan Siber, kami telah membuat *channel* dan *group* telegram secara khusus yang dapat digunakan berkomunikasi dengan mereka. Selain itu, BSSN juga telah menyelenggarakan

serangkaian pilot project, dan webinar yang berkaitan dengan pelaksanaan program ini.

7. **Bagaimana komitmen Tim ITSA terhadap proses kolaboratif dalam program ini?**

   Jawaban

   Komitmen kami mendukung 100%, hal ini bisa dilihat dari :

   a. Timeline penyusunan regulasi yang sangat singkat. Inisiasi penyusunan ini dimulai dari awal 2023, dan akhirnya bisa selesai 2023 serta ditetapkan oleh Kepala BSSN.
   b. Tim Itsa bersama pihak-pihak terkait di BSSN juga telah menyiapkan sumber daya, seperti SDM yang mengawaki, Platform / Aplikasi yang digunakan dalam penyelenggaraan program, dan tentunya yang mengawaki program ini tidak main-main. Semua pihak telah mendedikasikan untuk terlaksananya program ini.
   c. Pada Level Pimpinan, kita juga sudah memperjuangkan dari level bawah hingga pucuk pimpinan, dan semua sudah setujui.
   d. BSSN juga masih menjaga atau me-*maintance* hubungan baik dengan Bug Hunter / Komunitas / Pegiat Keamanan Siber dan PSE Lingkup Publik

8. **Bagaimana Tim ITSA menjaga hubungan internal dan eksternal untuk mendukung keberlangsungan proses kolaborasi?**

   Jawaban:

   Untuk menjaga hubungan yang baik secara internal Tim ITSA telah memiliki pemahaman yang akan tupoksi dan tanggunjawan masing-masing personil di Tim ITSA. Dengan berbekal kemampuan yang dimiliki oleh personil Tim ITSA yang mana secara keseluruhan adalah Lulusan dari Sekolah Tinggi Sandi Negara atau Politeknik Siber dan Sandi Negara. Sehingga tim telah dibekali dengan kemampuan yang cukup, sehingga kami percaya akan seluruh tim yang ada, dan dapat menjalankan tugas dan tanggung jawab sesuai kebutuhan organisasi.

   Selanjutnya secara ekternal dengan pihak-pihak lain seperti PSE Lingkup Publik, dan Pegiat Keamanan Siber, Tim ITSA juga telah membina hubungan

yang baik. Tim ITSA dengan PSE Lingkup Publik telah menjalin hubungan kerjasama di bidang identifikasi melalui layanan IT Security Assessment. Dan dengan Pegiat Keamanan Siber, kami telah membuat channel dan group khusus yang dapat digunakan berkomunikasi dengan mereka. Selain itu, Tim ITSA bersama BSSN juga telah menyelenggarakan serangkaian pilot project, dan webinar yang berkaitan dengan pelaksanaan program.

9. **Bagaimana Tim ITSA berpartisipasi dalam mencapai konsensus dalam menetapkan ruang lingkup pekerjaan dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawaban:

   Secara teknis Tim ITSA akan memberikan masukan dan melakukan kontrol terhadap pelaksaan pengujian sistem elektronik berdasarkan ruang lingkup yang telah diusulkan PSE Lingkup publik dan telah ditetapkan dalam program yang berjalan. Sehingga ketika terjadi pengujian sistem elektronik di luar ruang lingkup pengujian yang dilakukan oleh peserta pengidentifikasi kerentanan. Maka hal ini akan menjadikan laporan yang nantinya dikirimkan ke penyelenggara program dapat dinyatakan out-of-scoope dengan nilai minus, dan berdampak terhadap nilai akumulasi peserta tersebut.

   Dengan demikian, seluruh pihak yang terlibat dalam program harus benar-benar memperhatikan apa yang menjadi lingkup pekerjaan dari program yang telah ditetapkan.

10. **Bagaimana Tim ITSA mengelola pengetahuan yang didapat selama proses kolaborasi, terutama informasi kerentanan dari hasil pengujian?**

    Jawaban:

    Untuk mendapatkan pengetahuan yang cukup, kami akan menjalankan beberapa program melalui paltform dengan beberapa pilot project terkait penyelenggaraan program ini. Tentunya dalam jalannya akan ada evaluasi. Sehingga harapnya akan menjalankan secara efektif dan efisien. Evaluasi akan tetap dijalankan.

Ketika mendapatkan data kerentanan / statistik dan kumpulan data-data tersebut. Tidak hanya akan diolah menjadi himabuan keamanan, tapi ke depan akan didalami lebih lanjut sbg profile kerentanan berdasarkan sektor IIV.
Selanjutnya data yag dioleh dpt dijadikan rujukan untuk sektor-sektor tertentu. Namun demikian, data-data yang diproses merupakan data-data general untuk konsumsi publik atau data-data yang dijadikan sebagai bahan pengambilan keputusan sebagai upaya transpormasi digial.

11. **Bagaimana pendapat Anda terkait alokasi apresiasi terhadap peserta yang berprestasi dalam program ini?**

    Jawaban:

    Terkait apresiasi yang dialokasikan terhadap peserta yang berprestasi adalah sesuatu hal yang penting. Mengingat ini adalah salah satu faktor pendorong bagi para Pegiat keamanan siber untuk terlibat dan ingin mengikuti program ini. Selain itu apresiasi juga menandakan di level mana peserta tersebut dalam program ini. Semakin tinggi posisi peringkat yang didapatkan dari nilai-nilai pelaporannya, maka akan semakin besar juga peluang mendapatkan apresiasi yang bernilai tinggai bagi para peserta. Sehingga alokasi apresiasi pada program identifikasi kerentanan dan proteksi secara sukarela ini menjadi hal yang bisa dikatakan mutlak ada. Namun kembali lagi, ke prinsip dasar dari program, yaitu secara sukarela. Artinya peserta secara sadar dan rela berkenan untuk ikut dalam pelaksaan program ini, apapun bentuk apresiasinya. Namun BSSN juga perlu menetapkan standar yang tinggi, untuk menggaet para Pegiat keamanan siber agar berkontribusi dalam peningkatan keamanan siber di Indonesia.

12. **Apa pandangan Tim ITSA tentang akuntabilitas dalam penyelenggaraan program, terutama dalam konteks identifikasi kerentanan? Di sisi lain memungkinkan pengidentifikasi kerentanan tidak melaporkan seluruh kerentanan pada sistem elektronik yang diuji.**

    Jawaban:

    Dengan adanya mekanisme yang telah ditetapkan, semua entitas sudah diikat dengan perjanjian yang dapat mengikat, sehingga menjadi pembatas bagi hal-

hal yang tidak diinginkan. Namun dalam pelaksanaanya, memang seringkali memang terjadi hal-hal yang tidak diinginkan. Namun sekali lagi, adanya aturan bisa menjadi pembatas dan pengatur keselurahan entitas. Namun jika ada entitas ke 4 yg menjadi pengawas bisa meningkatkan penyelenggaran identifikasi kerentanan dan proteksi ini, seperti Aparat Penegak Hukum, asosiasi dkk.

13. **Bagaimana Tim ITSA menilai keberhasilan program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Adakah suatu indikator khusus dari sudut pandang tim ITSA?**

Jawaban:

Harapanya kami bisa berhasil, kita sudah melakukan riset untuk mebangun kegiatan ini. Paling tidak bisa menginisasi kegiatan lain, tidak hanya di sektor pemeritnah, tapi bisa juga di sektor lain. Selain itu, program ini juga dapat menjadi inisiasi untuk kegiatan lain, seperti pembinaan komunitas, dan pembinaan ekosistem siber lainnya.

Bisa jadi disektor industri bisa tumbuh kembang, terutama sektor industri keamanan siber, dan menjadikan pelaku insustri lebih bervariatif mulai dari alat yang diperjualbelikan, dan tidak hanya pihak itu-itu saja yang bermain di indusri ini.

Untuk menilai keberhasilan program ini, tim itsa juga telah menetapkan indikator khusus, seperti:

a. Timeline kegiatan, yang dibreakdown per thn/ smester, dengan target meningkat dalam kurun waktu tertenu misal thn pertama sekian bug hunter, sekian sistem elektronik, dan sekian PSE lingkup publik, dst.
b. VVIP masih lekat dengan BSSN, mulai dari pembiyaan dan penyelenggaraan. Kedepan memungkinkan bisa jadi program secara mandiri, terutama dari hal pembiayaan. Sehingga juga berdampak pada kompensasi yang lebih banyak untuk para Pegiat keamanan siber. Para pelaku industri keamanan siber juga berpeluang dalam memberikan dukungan pelaksanaan program ini.

Lampiran 3
Transkrip Wawancara 2

Ketua Tim Proteksi Direktorat Operasi Keamanan Siber

Narasumber	:	Indra Adi Putra, S.ST., M.M
Jabatan	:	Ketua Tim Proteksi, Direktorat Operasi Keamanan Siber
Unit Kerja	:	Direktorat Operasi Keamanan Siber, Deputi II BSSN
Tanggal	:	8 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Bagaimana keterlibatan Tim Proteksi terlibat dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Apakah dengan keterlibatan tersebut akan memperkaya pandangan dan pengetahuan, sehingga dapat menjadi solusi atas keamanan siber di sektor pemerintahan?**

   Jawaban:

   Tim Proteksi terlibat dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela dengan menjadi penyelenggara program tersebut. Melalui keterlibatan ini, kami memberikan kontribusi dalam menganalisis dan mengidentifikasi kerentanan pada sistem elektronik pemerintahan. Keterlibatan ini diharapkan dapat memperkaya pandangan dan pengetahuan kami dalam memahami berbagai ancaman keamanan siber yang mungkin terjadi di sektor pemerintahan, sehingga dapat memberikan solusi yang lebih efektif.

2. **Sebagai Ketua Tim Proteksi, bagaimana Anda mendukung dan memfasilitasi anggota tim dalam menjalankan program ini, dengan tidak meninggalkan tugas dan fungsi Tim Proteksi sehari-hari?**

   Jawaban:

   Sebagai Ketua Tim Proteksi, saya mendukung anggota tim dengan memberikan bimbingan dan sumber daya yang dibutuhkan untuk menjalankan program ini. Fasilitasi ini dilakukan tanpa meninggalkan tugas dan fungsi Tim Proteksi

sehari-hari, dengan memastikan bahwa anggota tim dapat melaksanakan tugasnya dengan efisien dan efektif.

3. **Apa tujuan bersama yang ingin dicapai oleh Tim Proteksi melalui program ini, khususnya dalam meningkatkan keamanan aplikasi SPBE melalui kegiatan identifikasi kerentanan?**

   Jawaban:

   Tujuan bersama yang ingin dicapai adalah meningkatkan keamanan aplikasi SPBE dengan melakukan identifikasi kerentanan, dan memastikan seluruh kerentanan dapat diremidiasi dan diperbaiki sebagaimana mestinya. Dengan demikian, dapat memberikan jaminan akan kerahasiaan, integritas dan ketersediaan sistem elektronik pemerintahan, menciptakan lingkungan yang lebih aman dan terlindungi dari ancaman siber

4. **Apakah ada aturan awal yang dijelaskan kepada anggota Tim Proteksi sebagai panduan dalam melaksanakan program Identifikasi Kerentanan dan Proteksi Secara Sukarela di konteks perlindungan sistem elektronik?**

   Jawaban:

   Aturan yang dijadikan rujukan dalam penyelenggaraan program ini adalah Peraturan Kepala Badan Siber Dan Sandi Negara Nomor 5 Tahun 2023 tentang Penyelenggaraan Program Identifikasi Kerentanan Dan Proteksi Secara Sukarela. Di dalam aturan tersebut, telah diatur ruang lingkup, hak, kewajiban, apresiasi, dan sanksi yang diberlakukan bagi peserta kegiatan.

5. **Bagaimana persepsi interdependensi antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber dalam menjalankan program ini? Bagaimana Anda melihat peran tim Proteksi dalam mencapai tujuan kolaboratif, terutama dalam konteks proteksi sistem elektronik?**

   Jawaban:

   Persepsi interdependensi antara BSSN, PSE Lingkup Publik, dan Pegiat keamanan siber sangat penting dalam menjalankan program ini. Tim Proteksi melihat dirinya sebagai elemen kunci dalam mencapai tujuan kolaboratif dengan memberikan kontribusi pada proteksi sistem elektronik, berkoordinasi

secara efektif dengan pihak terkait. BSSN berupaya untuk merangkul seluruh pihak untuk mengamankan sistem elektronik milik pemerintah. Kolaborasi ini dapat diwujudkan dari sisi Pegiat keamanan siber untuk melakukan pengujian kerentanan serta dari sisi PSE Lingkup Publik untuk melakukan penguatan sistem elektronik.

6. **Melihat sudah tersedianya standar teknis dan prosedur keamanan aplikasi SPBE, bagaimana keterkaitan dengan program ini?**

   Jawaban:

   Program ini dimaksudkan sebagai upaya percepatan implementasi atas standar teknis dan prosedur keamanan aplikasi SPBE yang telah ada. Standar teknis dan prosedur keamanan aplikasi SPBE sangat relevan dengan program ini. Tim Proteksi memastikan bahwa identifikasi kerentanan dan rekomendasi pengamanan yang dihasilkan sejalan dengan standar keamanan yang telah ditetapkan.

7. **Bagaimana upaya Tim Proteksi untuk membangun dan menjaga kepercayaan terhadap seluruh entitasi yang terlibat dalam penyelenggaraan program identifikasi kerentanan dan proteksi secara sukarela?**

   Jawaban:

   Tim Proteksi telah mengupayakan dalam membangun dan menjaga kepercayaan melibatkan transparansi dalam pelaksanaan program, komunikasi terbuka, dan konsistensi dalam penanganan temuan keamanan. Hal ini bertujuan untuk memastikan bahwa seluruh entitas yang terlibat merasa yakin dengan integritas dan tujuan dari program ini.

8. **Sejauh mana Tim Proteksi berkomitmen pada proses kolaboratif melalui program tersebut, kaitannya melindungi sistem elektronik atas ancaman siber yang semakin beragam?**

   Jawaban:

Tim Proteksi berkomitmen penuh pada proses kolaboratif melalui program ini, mengenali bahwa melindungi sistem elektronik dari ancaman siber memerlukan sinergi antara pemerintah dan masyarakat. Komitmen ini tercermin dalam partisipasi aktif dalam identifikasi kerentanan dan penerapan rekomendasi keamanan.

9. **Dalam menjalankan program kolaborasi, tentunya membutuhkan komitmen bersama dan hubungan yang baik antar semua aktor yang terlibat. Bagaimana upaya yang dilakukan Tim Proteksi, baik internal maupun eksternal untuk mendukung kelangsungan proses kolaborasi ini? Seperti upaya dalam kesepakatan ruang lingkup pekerjaan, aturan main, syarat dan ketentuan program terutama terkait perlindungan sistem elektronik?**

   Jawaban:

   Tim Proteksi berupaya untuk menjalin hubungan yang baik dengan semua pihak baik kepada PSE Lingkup Publik maupun Pegiat keamanan siber. Dari sisi PSE Lingkup Publik, Tim Proteksi telah menyediakan form yang dapat diisi oleh PSE Lingkup Publik terkait kesepakatan aplikasi yang akan diuji misalnya berapa banyak aplikasi, metode pengujian, serta *environment* aplikasi. Dari sisi Pegiat keamanan siber, BSSN berupaya untuk melakukan pengelolaan terhadap komunitas keamanan siber di luar sana agar dapat diberdayakan untuk kegiatan yang positif.

10. **Bagaimana strategi Tim Proteksi mengelola pengetahuan yang diperoleh selama proses kolaborasi, terutama dalam konteks bagaimana melakukan proteksi sistem elektronik berdasarkan rekomendasi pengamanan?**

    Jawaban:

    Strategi Tim Proteksi dalam mengelola pengetahuan melibatkan dokumentasi yang cermat, penyimpanan informasi yang aman, dan penggunaan database pengetahuan untuk menyimpan rekomendasi keamanan dan pengalaman yang diperoleh selama proses kolaborasi.

11. **Bagaimana pendapat Anda terkait alokasi apresiasi terhadap peserta yang berprestasi dalam program ini?**

    Jawaban:

    Kami memberikan apresiasi kepada peserta yang berprestasi dalam program ini melalui pengakuan publik, sertifikat penghargaan, atau mungkin insentif lainnya. Hal ini bertujuan untuk mendorong semangat dan dedikasi dalam meningkatkan keamanan sistem elektronik. Selain itu, kami juga memberikan kesempatan bagi PSE Lingkup Publik untuk berpartisipasi dalam pemberian apresiasi kepada peserta yang berprestasi pada program ini

12. **Apa pandangan Tim Proteksi tentang akuntabilitas dalam penyelenggaraan program, terutama dalam konteks Proteksi?**

    Jawaban:

    Tim Proteksi melihat akuntabilitas sebagai landasan penting dalam penyelenggaraan program ini. Setiap tindakan dan keputusan harus dapat dipertanggungjawabkan, sehingga dapat memastikan integritas dan keberlanjutan program.

13. **Bagaimana Tim Proteksi menilai keberhasilan program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Adakah suatu indikator khusus dari sudut pandang tim Proteksi?**

    Jawaban:

    Indikator utama dari keberhasilan program ini adalah menurunnya kasus serangan siber di Indonesia. Selain itu, indikator lain yang mendukung keberhasilan program Identifikasi Kerentanan dan Proteksi Secara Sukarela dinilai oleh Tim Proteksi melalui indikator seperti jumlah kerentanan yang berhasil diidentifikasi dan diperbaiki, tingkat kepatuhan terhadap standar keamanan, dan dampak positif terhadap keamanan sistem elektronik pemerintahan. Evaluasi ini memastikan bahwa program memberikan nilai tambah yang signifikan dalam melindungi aset informasi pemerintah.

Lampiran 4
Transkrip Wawancara 3

Pegiat Keamanan Siber

Narasumber : R. Setyawan
Jabatan : Pegiat Keamanan Siber
Tanggal : 7 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Sebagai Pegiat keamanan siber, apakah anda mengetahui program sejenis ini, dan bagaimana pendapat anda mengenai program yang diterbitkan oleh BSSN? Bagaimana mekanisme Pegiat keamanan siber untuk berpartisipasi dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawab:

   Saya sangat mengetahui program sejenis ini dan melihatnya sebagai langkah positif dari BSSN. Program Identifikasi Kerentanan dan Proteksi Secara Sukarela memberikan kesempatan bagi saya untuk berkontribusi langsung dalam meningkatkan keamanan aplikasi pemerintah. Adapun mekanisme untuk berpartisipasi biasanya melibatkan pendaftaran melalui platform atau kanal resmi yang disediakan oleh penyelenggara, diikuti dengan pengujian keamanan yang sesuai dengan aturan yang telah ditetapkan. Namun demikian perlu meningkatkan literasi dan publikasi terkait program ini, sehingga para pemilik sistem, komunitas dan masyarakat secara umum dapat mengetahui dan lebih banyak lagi yang berpartisipasi.

2. **Menurut pandangan Anda sebagai Pegiat keamanan siber, apa yang mendasari tujuan bersama dalam meningkatkan keamanan aplikasi pemerintah melalui program ini?**

   Jawab:

   Tujuan bersama yang mendasari adalah meningkatkan keamanan aplikasi pemerintah. Selain itu melalui program ini didorong oleh kebutuhan akan

perlindungan yang lebih baik terhadap sistem elektronik. Namun tidak semua Pegiat keamanan siber sudah memahami ini. Sebagai contoh para pencari bug / kerentanan yang masih muda seperti dikalangan siswa SMP, dan SMA perlu diberikan edukasi yang baik, sehingga mereka benar-benar paham bahwa pemerintah memiliki program yang serius. Saat ini para hacker baik di usia muda masih berada di kondisi mencari jati diri, mencari eksistensi, mencari ketenaran yang mana sering dilakukan dengan cara yang tidak baik seperti melakukan serangan web defacement di situs-situs pemerintah dan di situ memberikan beberapa kode, nama-nama hackernya.

Dengan demikian, Kolaborasi antara pemerintah dan Pegiat keamanan siber tidak hanya membantu mengidentifikasi kerentanan yang mungkin tidak terdeteksi secara internal, memperkuat lapisan keamanan, dan menciptakan ekosistem keamanan siber yang lebih tangguh. Namun juga sebagai wadah bagi pembinaan kepada masyarakat terutama kepada mereka-meraka yang memiki kemampuan di bidang keamanan siber untuk tidak menyalahgunakannya.

3. **Bagaimana respon Anda terhadap inisiatif BSSN terhadap program Identifikasi Kerentanan dan Proteksi Secara Sukarela yang akan segera dimulai?**

   Jawab:

   Saya menyambut baik inisiatif BSSN terhadap program Identifikasi Kerentanan dan Proteksi Secara Sukarela. Hal ini mencerminkan komitmen pemerintah dalam menghadapi tantangan keamanan siber dengan melibatkan para ahli dari masyarakat.

   Namun demikian perlu meningkatkan literasi dan publikasi terkait program ini, sehingga para pemilik sistem, komunitas dan masyarakat secara umum dapat mengetahui dan lebih banyak lagi yang berpartisipasi, serta apresiasi yang tepat sebagai nilai jual lebih.

4. **Berdasarkan pengalaman Anda, Apakah Anda memiliki pengetahuan tentang aturan awal (*preliminary rules*) yang dijadikan acuan dalam mengikuti program serupa Identifikasi Kerentanan dan/atau Proteksi Secara Sukarela?**

   Jawab:

   Aturan awal (*preliminary rules*) biasanya dijelaskan oleh penyelenggara program, mencakup pedoman etika, batasan pengujian, dan mekanisme pelaporan hasil temuan. Sebagai Pegiat keamanan siber, memahami aturan ini penting sebelum berpartisipasi dalam program.

5. **Dalam melakukan kolaborasi pemerintah dan masyarakat, Bagaimana Anda sebagai Pegiat keamanan siber memandang pentingnya hubungan saling ketergantungan antara seluruh pihak yang terlibat dalam program ini?**

   Jawab:

   Hubungan saling ketergantungan antara semua pihak terlibat sangat penting dalam program ini. Saya memandang pentingnya kolaborasi untuk memahami secara menyeluruh ancaman dan kerentanan yang ada, serta merumuskan solusi yang efektif.

   Selain itu dari sisi Pegiat keamanan siber kita memandang perlunya adanya langkah kongkrit yang diambil para pemilik sistem yang berasal dari instansi pemerintah. Dari beberapa berdiskusi dengan para Pegiat yang melaporkan kerentanan kepada instansi-instansi tersebut hanya mendapatkan respon "**baik terimakasih kasih mas**" namun tidak melakukan aksi yang tepat, sehingga kerentanan sistem tersebut tidak benar-benar ditutup secara cepat. Hal ini tentunya akan mengkhawatirkan keadaan sistem tersebut dan diakhirnya nanti mungkin akan berdampak terhadap citra organisasi. Ini kaitannya juga dengan wibawa pimpinan di organisasi tersebut. Dari pengalaman tidak sedikit Kepala Unit TIK yang belum memiliki kesadaran keamanan siber yang baik.

   Penting untuk melihat peran masing-masing lagi sesuai tugas dan tanggung jawab pada proses kolaborasi ini. Sebagai Pegiat kami juga ingin membantu pemerintah untuk meningkatkan keamanan sibernya.

6. **Apakah Anda memberikan investasi awal untuk mengikuti program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Seperti biaya pendaftaran, atau investasi dalam bentuk lain. Berkenan anda dapat menjelaskan secara lengkap.**

   Jawab:

   Sebagai Pegiat keamanan siber, investasi awal seperti biaya pendaftaran biasanya dianggap sebagai investasi dalam pengembangan keamanan siber dan keberlanjutan program ini. Selain itu, saya juga telah mengembangkan kompetensi diri dengan mengikuti pelatihan serta sertifikasi terkait keamanan siber. Namun, seiring dengan kontribusi yang diberikan, apresiasi dalam bentuk uang tunai, souvenir, atau sertifikat juga dapat diharapkan. Hal ini akan menjadi penyemangat bagi kami untuk berpartisipasi pada program-program seperti ini. terlebih lagi program identifikasi kerentanan yang sifatnya sukarela, jika tidak memiliki apresiasi yang jelas akan kurang diminati di kalangan Pegiat keamanan siber yang sudah memiliki jam terbang tinggi. Mereka akan mempertimbangkan program-program yang menghasilkan bounty / apresiasi yang besar.

7. **Untuk menjamin terselenggaranya program Identifikasi kerentanan dan Proteksi Secara Sukarela dibutuhkan komitmen bersama antar seluruh entitias yang terlibat, baik dari penyelenggara, pemilik sistem elektronik, dan para Pegiat keamanan siber.**

   Apakah Anda memiliki komitmen terhadap proses kolaboratif dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?

   Jawab:

   Jika program ini berjalan, maka Saya memiliki komitmen penuh terhadap proses kolaboratif dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela. Kolaborasi ini penting untuk mencapai tujuan bersama dalam meningkatkan keamanan sistem elektronik pemerintah. Bagi kami yang memiliki kepedulian terhadap kondisi ekosistem keamanan siber di Indonesia membutuhkan program-program seperti ini dan tentunya melalui koordinasi dari pemerintah. Namun demikian perlu meningkatkan literasi dan publikasi

terkait program ini, sehingga para pemilik sistem, komunitas dan masyarakat secara umum dapat mengetahui dan lebih banyak lagi yang berpartisipasi.

8. **Bagaimana Anda selaku Pegiat keamanan siber dapat membangun kepercayaan dengan seluruh aktor yang terlibat dalam program ini? Adakah klausul / prasyarat yang dapat dijadikan acuan?**

   Jawab:

   Saya berharap adanya upaya untuk membangun kepercayaan melibatkan transparansi, komunikasi terbuka, dan pemenuhan kewajiban yang diatur dalam aturan program. Klausul atau prasyarat tertentu dapat dijadikan acuan untuk memastikan integritas dan keamanan informasi. Dengan adanya hal tersebut dapat memperkuat pelaksanaan dan kepatuhan oleh pihak-pihak yang terlibat terhadap peraturan yang ada.

9. **Berdasarkan pengalaman Anda, apakah anda pernah bekerjasama dengan instansi pemerintah? Jika pernah, bagaimana anda menjaga hubungan tersebut jika dikaitkan dengan program yang ditetapkan oleh BSSN untuk mendukung keberlangsungan proses kolaborasi?**

   Jawab:

   Saya pernah bekerjasama dengan instansi pemerintah dalam program serupa. Untuk menjaga hubungan tersebut, komunikasi terbuka, penghormatan terhadap aturan program, dan pemahaman mendalam terhadap tujuan bersama sangat penting.

10. **Dalam melaksanakan identifikasi kerentanan dan/atau memberikan rekomendasi proteksi dibutuhkan ruang lingkup yang jelas dan tepat. Apakah anda selaku Pegiat keamanan siber dapat memutuskan bahwa anda sepakat dengan ruang lingkup pekerjaan dalam program yang diselenggarakan?**

    Jawab:

    Sebagai Pegiat keamanan siber, penting untuk memastikan bahwa ruang lingkup pekerjaan dalam program sesuai dengan keahlian dan kemampuan saya.

Keterlibatan dalam tahapan perencanaan dan definisi ruang lingkup dapat membantu untuk memastikan kesesuaian scope pekerjaan yang saya lakukan.

11. **Ketika anda mengikuti program Identifikasi kerentanan dan proteksi secara sukarela, tentunya mendapatkan berbagai informasi sensitif terkait kerentanan dan sistem elektronik terkait, dan memungkinkan mendapatkan informasi sensitif lainnya seperti data pribadi. Bagaimana Anda selaku Pegiat keamanan siber mengelola pengetahuan yang didapat selama proses kolaborasi?**

    Jawab:

    Pengelolaan pengetahuan melibatkan dokumentasi yang cermat, penyimpanan informasi yang aman, dan kepatuhan terhadap kebijakan privasi. Saya akan memastikan bahwa informasi sensitif dikelola dengan aman dan hanya diakses oleh pihak yang berwenang. Tentunya apabila data yang saya dapatkan dari sebuah celah kerentanan merupakan data sensitif, saya akan bertindak secara etis untuk tidak menyimpan, mempublikasikan, maupun membocorkan data tersebut sesuai dengan kesepakatan perjanjian yang telah saya tandatangani, biasanya ada dokumen perjanjian kerahasiaan seperti *Non-Dosclosure Agreement*.

12. **Dari program yang anda ikuti, apakah penyelenggara dan/atau pemilik sistem elektronik memberikan hak-hak apresiasi berdasarkan kontribusi anda ?**

    Jawab:

    Penyelenggara dan/atau pemilik sistem elektronik memberikan hak apresiasi berdasarkan kontribusi saya dalam bentuk penghargaan publik, sertifikat, atau imbalan lainnya.

13. **Jika dalam pelaksanaannya, Anda berhasil menemukan kerentanan lain terkait ruang lingkup pengujian pada media online sumber terbuka (*open source*) baik berupa dugaan kebocoran data, atau informasi sensitif lainnya. Apa langkah yang Anda ambil sebagai bentuk komitmen anda untuk menjadi Hacker Baik?**

    Jawab:

    Saya bersedia melaporkan temuan tambahan terkait keamanan pada media online sumber terbuka sebagai bentuk komitmen sebagai Hacker Baik. Hal ini dapat mempercepat dalam membantu pemilik sistem untuk melakukan tindakan reaktif dari temuan tersebut.

14. **Bagaimana Anda menilai program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil?**

    Jawab:

    Keberhasilan program Identifikasi Kerentanan dan Proteksi Secara Sukarela dapat diukur oleh sejauh mana kerentanan berhasil diidentifikasi dan diperbaiki, tingkat partisipasi Pegiat keamanan siber, dan dampak positif terhadap keamanan sistem elektronik pemerintah. Evaluasi ini dapat memberikan pandangan secara menyeluruh terhadap efektivitas program. Dengan demikian, harapannya dapat membawa keberhasilan pelaksanaan program ini.

Lampiran 5
Transkrip Wawancara 4

Pegiat Keamanan Siber

Narasumber : R. Sandya
Jabatan : Pegiat Keamanan Siber
Tanggal : 29 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Sebagai praktisi keamanan siber, apakah anda mengetahui program sejenis ini, dan bagaimana pendapat anda mengenai program yang diterbitkan oleh BSSN? Bagaimana mekanisme praktisi keamanan siber untuk berpartisipasi dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawab:

   Ya, beberapa program yang saya ketahui seperti Bugcrowd, dan Hacker One juga menyediakan program sukarela dengan hadiah berupa poin tidak hanya uang. Pada program tersebut partisipasi sangat mudah, mengisi formulir pendaftaran dan menyediakan informasi dasar mengenai diri kita untuk dilengkapi ketika sudah mendapatkan konfirmasi email pendaftaran.

2. **Menurut pandangan Anda sebagai praktisi keamanan siber, apa yang mendasari tujuan bersama dalam meningkatkan keamanan aplikasi pemerintah melalui program ini?**

   Jawab:

   Menurut saya pribadi, dasar dari kegiatan ini ialah adanya peningkatan atas kesadaran keamanan siber di Indonesia, apalagi setelah kita tahu kalau beberapa instansi mengalami kebocoran data, sebut saja yang paling heboh ialah ketika BPJS dan KPU mengalami kebocoran. Dari situ timbul juga motivasi saya untuk melakukan pengamanan sistem secara sukarela, terutama bagi Indonesia, karena data saya juga disimpan di Indonesia.

3. **Bagaimana respon Anda terhadap inisiatif BSSN terhadap program Identifikasi Kerentanan dan Proteksi Secara Sukarela yang akan segera dimulai?**

   Jawab:

   Saya sangat apresiasi niatan BSSN menciptakan program ini, ketika mendengar informasi mengenai program ini, saya sebagai masyarakat merasa diakui dengan disediakannya wadah bagi saya untuk menyalurkan niat baik saya.

4. **Berdasarkan pengalaman Anda, Apakah Anda memiliki pengetahuan tentang aturan awal (*preliminary rules*) yang dijadikan acuan dalam mengikuti program serupa Identifikasi Kerentanan dan/atau Proteksi Secara Sukarela?**

   Jawab:

   Ya, meski berbeda beda setiap platform, namun aturan awal dari setiap program sukarela ini biasanya mencakup kerahasiaan, etika, dan keamanan sistem itu sendiri.

5. **Dalam melakukan kolaborasi pemerintah dan masyarakat, Bagaimana Anda sebagai praktisi keamanan siber memandang pentingnya hubungan saling ketergantungan antara seluruh pihak yang terlibat dalam program ini?**

   Jawab:

   Menurut hemat saya, dengan banyaknya sistem digital yang dibuat oleh pemerintah serta banyaknya kebocoran data, timbul urgensi dari pemerintah untuk mengamankan sistem elektronik yang dibuat, hal ini tentunya tidak akan dapat dipenuhi oleh BSSN sendirian. Masyarakat dan praktisi dengan segudang prestasi di lomba keamanan siber pun mulai bermunculan dari Indonesia, potensi ini tentu akan menjadi sia-sia dan tidak akan berkembang apabila pemerintah tidak memberikan sebuah wadah yang proporsional. Oleh karena itu, muncullah sebuah hubungan saling ketergantungan antara PSE dengan BSSN, BSSN dengan masyarakat dan praktisi keamanan siber, serta PSE dengan masyarakat dan praktisi keamanan siber.

6. **Apakah Anda memberikan investasi awal untuk mengikuti program Identifikasi Kerentanan dan Proteksi Secara Sukarela? Seperti biaya pendaftaran, atau investasi dalam bentuk lain. Berkenan anda dapat menjelaskan secara lengkap.**

   Jawab:

   Investasi yang saya lakukan ialah dengan membeli VPS sendiri serta lisensi *tools*, seperti burpsuite dan IDAPro.Untuk menjamin terselenggaranya program Identifikasi kerentanan dan Proteksi Secara Sukarela dibutuhkan komitmen bersama antar seluruh entitias yang terlibat, baik dari penyelenggara, pemilik sistem elektronik, dan para praktisi keamanan siber.

7. **Apakah Anda memiliki komitmen terhadap proses kolaboratif dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawab:

   Ya, saya memiliki komitmen penuh untuk ikut berkolaborasi dalam program ini, hal ini karena saya telah berkomitmen untuk melakukan pengamanan siber bagi pemerintah secara sukarela dan memenuhi portofolio saya dengan hal tersebut.

8. **Bagaimana Anda selaku praktisi keamanan siber dapat membangun kepercayaan dengan seluruh aktor yang terlibat dalam program ini? Adakah klausul / prasyarat yang dapat dijadikan acuan?**

   Jawab:

   Saya bersedia untuk mengisi NDA dan nota kesepahaman lainnya dengan data pribadi saya yang dijamin keasliannya. Setelah *report* saya kirimkan saya juga hanya akan mempublikasikan *report* tersebut apabila mendapat persetujuan pemilik sistem, tentunya dengan menutupi path atau parameter aslinya.

9. **Berdasarkan pengalaman Anda, apakah anda pernah bekerjasama dengan instansi pemerintah? Jika pernah, bagaimana anda menjaga hubungan tersebut jika dikaitkan dengan program yang ditetapkan oleh BSSN untuk mendukung keberlangsungan proses kolaborasi?**

   Jawab:

   Saya pernah menjalani kerjasama dengan salah satu Diskominfo di pulau Jawa dalam pelaksanaan magang saya. Magang pertama saya diminta untuk melakukan verifikasi hasil *vulnerablity scanning* yang merupakan agenda rutin dari Diskominfo tersebut terhadap aplikasi di daerahnya. Dalam menjaga hubungan tersebut saya berusaha memberikan yang terbaik pada saat pelaksanaan dan ikut bergabung dengan komunitas yang telah disediakan oleh Diskominfo tersebut guna tetap berkontribusi apabila terdapat sistem baru yang dibuat.

10. **Dalam melaksanakan identifikasi kerentanan dan/atau memberikan rekomendasi proteksi dibutuhkan ruang lingkup yang jelas dan tepat. Apakah anda selaku praktisi keamanan siber dapat memutuskan bahwa anda sepakat dengan ruang lingkup pekerjaan dalam program yang diselenggarakan?**

    Jawab:

    Ya, Kami dapat memutuskan sepakat atau tidaknya dengan ruang lingkup pekerjaan yang diberikan, dan kami dapat mencari program lain apabila program tersebut tidak sesuai dengan ruang lingkup pekerjaan kami.

11. **Ketika anda mengikuti program Identifikasi kerentanan dan proteksi secara sukarela, tentunya mendapatkan berbagai informasi sensitif terkait kerentanan dan sistem elektronik terkait, dan memungkinkan mendapatkan informasi sensitif lainnya seperti data pribadi. Bagaimana Anda selaku praktisi keamanan siber mengelola pengetahuan yang didapat selama proses kolaborasi?**

    Jawab:

Seluruh data yang telah terekstrak pada saat proses pengujian tidak akan diperjualbelikan dan langsung dihapus ketika telah terdapat informasi bahwanya pengamanan telah dilakukan.

12. **Dari program yang anda ikuti, apakah penyelenggara dan/atau pemilik sistem elektronik memberikan hak-hak apresiasi berdasarkan kontribusi anda ?**

    Jawab:

    Ya, mereka memberi hak apresiasi terhadap Saya berdasarakan tingkat dampak yang telah saya temukan.

13. **Jika dalam pelaksanaannya, Anda berhasil menemukan kerentanan lain terkait ruang lingkup pengujian pada media online sumber terbuka (*open source*) baik berupa dugaan kebocoran data, atau informasi sensitif lainnya. Apakah anda bersedia untuk melaporkan ke penyelenggara program dan/atau pemilik sistem elektronik sebagai bentuk komitmen anda untuk menjadi Hacker Baik?**

    Jawab:

    Ya, Saya akan melaporkannya agar tidak ada percobaan masuk setelah data bocor menggunakan kredensial untuk masuk mengalami kebocoran

14. **Bagaimana Anda menilai program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil?**

    Jawab: :

    Program Identifikasi Kerentanan dan Proteksi secara sukarela berhasil ketika kolaborasi tetap berjalan hingga berkembang dengan mekanisme yang lebih efektif dan hadiah hadiah yang lebih menarik ke depannya sehingga animo masyarakat tidak akan berkurang

Lampiran 6 Transkrip Wawancara 5

PSE Lingkup Publik

Narasumber : Ryandi Yusuf

Peran : PSE Lingkup Publik – Kejaksaan Agung

Tanggal : 30 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Dengan adanya program kolaborasi yang ditetapkan BSSN, apakah organisasi anda selaku PSE Lingkup publik memungkinkan berpartisipasi dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela?**

   Jawaban:

   Memungkinkan

2. **Menurut pandangan Anda, hal apa yang mendasari tujuan kolaborasi melalui program ini jika dikaitkan dengan implementasi keamanan siber di organisasi anda?**

   Jawaban:

   Tujuan kolaborasi pada program ini sejalan dengan tujuan dari keamanan siber pada organisasi kami, yaitu dalam penegakan hukum. Tujuan organisasi kami tentunya dalam rangka menghadirkan kepastian hukum serta melindungi kepentingan umum di bidang penegakan hukum. Sehingga jika terjadi suatu serangan siber yang dapat mengganggu kinerja organisasi kami, tentunya tujuan awal akan mengalami hambatan serta berdampak terhadap penurunan kepercayaan masyarakat terhadap organisasi kami.

3. **Menurut pandangan Anda, bagaimana Organisasi Anda akan memberikan respon terhadap rencana BSSN dalam menyelenggarakan program Identifikasi Kerentanan dan Proteksi Secara Sukarela ini?**

   Jawaban:

   Organisasi kami tentunya akan menjalin koordinasi dan partisipasi aktif serta keikutsertaan dalam membangun dan mendukung program ini dengan BSSN

sebagai pusatnya. Kami meyakini bahwa keberhasilan program ini bukan hanya berada di pihak BSSN saja, tetapi seluruh pengguna, termasuk organisasi kami yang terlibat di dalamnya.

4. **Berdasarkan kondisi yang ada, apakah organisasi anda telah memiliki aturan awal (*preliminary rules*) yang dijadikan acuan dalam dalam penyelenggaraan program serupa (jika ada), baik dalam hal identifikasi kerentanan maupun pemberian rekomendasi pengamanan?**

   Jawaban:

   Saat ini acuan penyelenggaraan program di organisasi kami belum dituangkan ke dalam peraturan, dan masih dalam proses pengusulan, sehingga segala bentuk acuan masih berpegangan pada aturan di BSSN.

5. **Bagaimana organisasi Anda menyikapi proses kolaborasi ini? Apakah terlihat adanya potensi saling membutuhkan diantara seluruh pihak yang terlibat dalam kolaborasi? Baik dari BSSN, para pegiat keamanan siber, maupun Organisasi Anda?**

   Jawaban:

   Organisasi kami menilai bahwa keterlibatan seluruh elemen di dalam program ini menjadi kunci keberhasilan dari program kolaborasi ini. Di internal organisasi, peran pelaksana hingga pimpinan menjadi penting dalam menjalankan program kolaborasi, sedangkan di eksternal organisasi, komunikasi dan koordinasi menjadi jembatan yang penting untuk menciptakan suatu ikatan keterkaitan antara bssn selaku organisasi induk dengan organisasi kami sebagai pengguna.

6. **Selain dukungan kebijakan, apakah organisasi Anda memandang bahwa dukungan dalam bentuk investasi jenis lain yang dapat diberikan sebagai bentuk apresiasi kepada praktisi keamanan siber untuk mendukung keberhasilan program tersebut? Jika iya terdapat investasi jenis lain, maka jenis investasi apa yang akan diberikan?**

   Jawaban:

Organisasi kami memandang bahwa kebijakan memberikan suatu kepastian terhadap keberlangsungan program tersebut, sedangkan dukungan anggaran (operasional, reward/penghargaan, dan dukungan lain) merupakan bentuk nyata terhadap dukungan dan keseriusan terhadap program tersebut. Adapun investasi lainnya pada program tersebut berbentuk kolaborasi dan penunjukan sebagai narasumber maupun sebagai konsultan, sehingga memberikan dukungan dalam bentuk nyata yang diakui oleh negara dalam hal pertanggungjawaban anggaran.

7. **Jika organisasi Anda berminat mengikuti program identifikasi dan kerentanan secara sukarela (VVIP BSSN), bagaimana komitmen organisasi anda terhadap proses kolaboratif melalui program ini?**

   Jawaban:

   Komitmen organisasi kami dalam mengikuti program VVIP tersebut tentunya berawal dari koordinasi dan komunikasi aktif dengan BSSN dalam pembentukan pondasi awal pada program tersebut, sehingga hal-hal yang menjadi dasar program tersebut tidak terlewatkan.

8. **Selanjutnya dari pengalaman Anda, Bagaimana organisasi anda dapat membangun kepercayaan dengan seluruh pihak yang terlibat dalam program ini? baik dari BSSN maupun dengan para pegiat keamanan siber?**

   Jawaban:

   Dengan komunikasi aktif, baik secara langsung maupun tidak langsung, serta penyampaian informasi di saluran resmi organisasi dengan memberikan suatu pemberitaan dan penyampaian reward dalam bentuk investasi lainnya sehingga dapat menggugah keikutsertaan dari pihak eksternal dalam mensukseskan program tersebut.

9. **Berdasarkan pengalaman, bagaimana organisasi Anda menjaga hubungan internal dan eksternal untuk mendukung keberlangsungan proses kolaborasi?**

   Jawaban:

   Di internal, pengalaman organisasi kami di level pimpinan memang mengalami kendala, karena tupoksi mengenai kemanan siber belum menjadi perhatian pimpinan organisasi, baik di level daerah maupun di level pusat, sehingga pengajuan program, baik dari kebijakan hingga dukungan anggaran mengalami keterlambatan dalam penyelesaiannya. Namun dari level pelaksana, pemahaman mengenai program VVIP menjadi topik utama yang menjadi bagian penting terhadap perlindungan keamanan siber yang ada di organisasi, sehingga jalan keluar dari permasalahan tersebut adalah adanya komunikasi yang efektif yang disampaikan kepada pimpinan organisasi.

   Di eksternal, pengalaman organisasi kami sebenarnya belum bersinggungan dengan pihak di luar pemerintahan. Sehingga yang terjadi saat ini adalah keterikatan dengan BSSN selaku organisasi pemerintah yang membidangi permasalahan keamanan informasi dan keamanan siber.

10. **Pada saat mendaftarkan diri untuk mengikuti program identifikasi kerentanan dan proteksi secara sukarela, Bagaimana organisasi Anda menetapkan ruang lingkup yang dikerjakan telah sesuai dengan harapan Anda? Apakah terdapat koordinasi antar seluruh pihak yang terlibat dalam program kolaborasi?**

    Jawaban:

    Organisasi kami menetapkan fungsi dan kewenangan pihak-pihak yang terlibat di dalam program VVIP tersebut, selanjutnya menetapkan jalur koordinasi sehingga komunikasi dapat berjalan secara efektif ketika program telah dijalankan.

11. **Menurut pandangan Anda, bagaimana langkah organisasi Anda dalam mengelola pengetahuan yang didapat dari proses kolaborasi?**

    Jawaban:

Organisasi kami menilai saat ini, pengetahuan mengenai tujuan program VVIP ini masih terbatas di satuan kerja yang membidangi keamanan informasi dan keamanan siber yang ada di Organisasi kami, sehingga belum seluruh satuan kerja yang ada di organisasi kami memahami dengan baik tujuan dan manfaat dari program VVIP tersebut. Oleh sebab itu, masih banyaknya tugas dan pekerjaan rumah (PR) yang harus dilakukan oleh Organisasi kami agar pengetahuan dan informasi tersebut dapat diterima di seluruh satuan kerja.

12. **Menurut pandangan Anda, apakah seluruh pihak telah menerima manfaat berdasarkan investasi yang telah dilakukan dalam program identifikasi dan kerentanan secara sukarela ini?**
    Jawaban:
    Belum seluruhnya

13. **Menurut pandangan Anda, apakah dalam penyeleggaraan program ini telah menerapkan asas transparansi dan akuntabilitas?**
    Jawaban:
    Belum dapat menilai bahwa asas transparansi dan akuntabilitas telah hadir dalam penyelenggaraan program VVIP tersebut dikarenakan belum berjalannya program VVIP tersebut di organisasi kami.

14. **Menurut pengalaman Anda, bagaimana organisasi Anda menilai program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil?**
    Jawaban:
    Organisasi kami menilai bahwa program VVIP tersebut dapat dikatakan berhasil jika seluruh dukungan dari pihak-pihak yang terlibat, baik internal maupun eksternal dapat berjalan sesuai dengan fungsinya, ditambah dengan adanya koordinasi aktif sehingga seluruh pihak dapat terlibat dan merasa memiliki program VVIP tersebut.

Lampiran 7
Transkrip Wawancara 6

Pegiat Keamanan Siber

Narasumber : Subroto Budhi Utomo
Peran : PSE Lingkup Publik – Jawa Tengah
Tanggal : 28 Januari 2024

Hasil Wawancara dengan Narasumber

1. **Dengan adanya program kolaborasi yang ditetapkan BSSN seperti VVIP Program, apakah organisasi anda selaku PSE Lingkup publik memungkinkan berpartisipasi dalam program Identifikasi Kerentanan dan Proteksi Secara Sukarela ?**

   Jawaban

   Sangat mungkin sekali kami akan berpartisipasi dalam program tersebut.

2. **Menurut pandangan Anda, hal apa yang mendasari tujuan kolaborasi melalui program ini jika dikaitkan dengan implementasi keamanan siber di organisasi anda?**

   Jawaban

   Program kolaborasi ini akan sangat membantu meningkatkan keamanan sistem elektronik dan aplikasi milik Pemerintah Provinsi Jawa Tengah. Karena dengan adanya program ini dapat di deteksi kemungkinan ada kerentanan keamanan yang tidak terdeteksi oleh tim internal. Selain itu program ini diharapkan dapat meningkatkan respon terhadap ancaman siber yang semakin meningkat.

3. **Menurut pandangan Anda, bagaimana Organisasi Anda akan memberikan respon terhadap rencana BSSN dalam menyelenggarakan program Identifikasi Kerentanan dan Proteksi Secara Sukarela ini ?**

   Jawaban

   Pemerintah Provinsi Jawa Tengah sangat merespon secara positif dengan adanya program ini, dikarenakan manfaat dari program ini yang dapat membantu dalam mendeteksi adanya kerentanan pada sistem serta bagaimana melakukan mitigasinya.

4. **Berdasarkan kondisi yang ada, apakah organisasi anda telah memiliki aturan awal (preliminary rules) yang dijadikan acuan dalam dalam penyelenggaraan program serupa (jika ada), baik dalam hal identifikasi kerentanan maupun pemberian rekomendasi pengamanan yang bekerjasama dengan pihak eksternal organisasi?**

   Jawaban

   Secara tertulis, Pemerintah Provinsi Jawa Tengah belum memiliki preliminary rules dalam penyelenggaraan serupa, namun kami telah menerapkan aturan-aturan yang tidak tertulis / best practise dalam menerima pengaduan/pelaporan mengenai temuan celah keamanan pada sistem/aplikasi dari masyarakat.

5. **Bagaimana organisasi Anda menyikapi proses kolaborasi ini? Apakah terlihat adanya potensi saling membutuhkan diantara seluruh pihak yang terlibat dalam kolaborasi? Baik dari BSSN, para pegiat keamanan siber, maupun Organisasi Anda?**

   Jawaban

   Dengan adanya kolaborasi ini maka diharapkan semua pihak dapat memperoleh keuntungan / mutualisme seperti pihak PSE dapat mengetahui adanya celah keamanan pada sistem, penggiat keamanan siber dapat menyalurkan bakatnya secara legal tanpa harus khawatir adanya konsekuensi hukum serta mendapatkan reward baik berupa material maupun immaterial, selain itu BSSN juga dapat memonitor dan mengarahkan penggiat siber untuk tujuan yang baik dan meminimalisir terjadinya insiden siber yang dikarenakan adanya penggiat keamanan siber yang melakukan serangan terhadap sistem/aplikasi yang sudah berjalan.

6. **Selain dukungan kebijakan, apakah organisasi Anda memandang bahwa dukungan dalam bentuk investasi jenis lain yang dapat diberikan sebagai bentuk apresiasi kepada praktisi keamanan siber untuk mendukung keberhasilan program tersebut?**

   Jika iya terdapat investasi jenis lain, maka jenis investasi apa yang akan diberikan?

   Jawaban

Organisasi dapat mengalokasikan dana untuk menjadikan praktisi keamanan siber sebagai narasumber ataupun pelatih bagi tim keamanan siber organisasi agar dapat terus meningkatkan keterampilan dan pengetahuan mereka. Selain itu, Organisasi dapat menyediakan kesempatan bagi para bug hunter untuk berkolaborasi dengan tim keamanan siber organisasi dalam proyek-proyek penelitian keamanan atau pengembangan alat keamanan baru. Hal ini tidak hanya memberikan manfaat bagi organisasi dalam meningkatkan keamanan mereka, tetapi juga memberikan kesempatan bagi para bug hunter untuk memperluas jaringan mereka dan mendapatkan pengalaman yang berharga.

7. **Jika organisasi Anda berminat mengikuti program identifikasi dan kerentanan secara sukarela (VVIP BSSN), bagaimana komitmen organisasi anda terhadap proses kolaboratif melalui program ini?**

   Jawaban

   Kami akan segera menindak lanjuti temuan kerentanan pada sistem elektronik milik Pemerintah Provinsi Jawa Tengah dengan melakukan perbaikan dan penutupan celah keamanan sesuai rekomendasi.

8. **Selanjutnya dari pengalaman Anda, Bagaimana organisasi anda dapat membangun kepercayaan dengan seluruh pihak yang terlibat dalam program ini? baik dari BSSN maupun dengan para pegiat keamanan siber?**

   Jawaban

   - Menerapkan Non Disclosure Agreement dalam setiap kegiatan, Organisasi harus memastikan bahwa mereka mematuhi semua regulasi dan standar keamanan yang relevan. Ini termasuk regulasi terkait perlindungan data pribadi, standar keamanan jaringan, dan persyaratan pelaporan insiden keamanan.
   - Penyelenggara harus Memberikan Pengakuan dan Apresiasi, berupa pengakuan dan menghargai kontribusi yang diberikan oleh para praktisi keamanan siber dalam meningkatkan keamanan organisasi. Ini dapat dilakukan melalui penghargaan resmi, pengakuan publik, atau kesempatan untuk berkolaborasi secara lebih dalam dalam program keamanan siber.

9. **Berdasarkan pengalaman, bagaimana organisasi Anda menjaga hubungan internal dan eksternal untuk mendukung keberlangsungan proses kolaborasi?**

   Jawaban

   Untuk menjaga hubungan dalam mendukung keberlangsungan kolaborasi dibentuklah sebuah grup/perkumpulan serta sering dilakukan tukar pikiran dalam membahas sebuah kasus yang hangat, selain itu melakukan pertemuan rutin dan berbagi informasi juga dapat meningkatkan kolaborasi.

10. **Pada saat mendaftarkan diri untuk mengikuti program identifikasi kerentanan dan proteksi secara sukarela, Bagaimana organisasi Anda menetapkan ruang lingkup yang dikerjakan telah sesuai dengan harapan Anda? Apakah terdapat koordinasi antar seluruh pihak yang terlibat dalam program kolaborasi?**

    Jawaban

    Sebelum pelaksanaan program dilakukan koordinasi terlebih dahulu dengan pemilik Sistem Elektronik yang akan dijadikan target untuk mengetahui cara kerja, mempersiapkan data dummy serta kredensial pengujian, selain itu dilakukan duplikasi terhadap sistem dan ditempatkan pada lingkungan khusus pengujian. Hal ini perlu dilakukan agar pengujian dapat berlangsung secara maksimal dan tidak keluar dari ruang lingkup pengujian yang sudah ditetapkan.

11. **Menurut pandangan Anda, bagaimana langkah organisasi Anda dalam mengelola pengetahuan yang didapat dari proses kolaborasi?**

    Jawaban

    Dilakukan PoC ulang terhadap temuan yang diberikan oleh para peserta, selain itu kami melakukan dokumentasi terhadap PoC yang telah kami dapatkan, sehingga dapat dijadikan sebagai ilmu pembelajaran bagi kami.

12. **Menurut pandangan Anda, apakah seluruh pihak telah menerima manfaat berdasarkan investasi yang telah dilakukan dalam program identifikasi dan kerentanan secara sukarela ini?**

    Jawaban

    Seluruh pihak telah menerima manfaat program ini, pihak PSE dapat mengetahui adanya celah keamanan pada sistem, penggiat keamanan siber

dapat menyalurkan bakatnya secara legal tanpa harus khawatir adanya konsekuensi hukum serta mendapatkan reward baik berupa material maupun immaterial, selain itu BSSN juga dapat memonitor dan mengarahkan penggiat siber untuk tujuan yang baik dan meminimalisir terjadinya insiden siber yang dikarenakan adanya penggiat keamanan siber yang melakukan serangan terhadap sistem/aplikasi yang sudah berjalan.

13. **Menurut pandangan Anda, apakah dalam penyelenggaraan program ini telah menerapkan asas transparansi dan akuntabilitas?**

    Jawaban

    Dalam pelaksanaan program ini telah diterapkan asas transparansi, kami selaku PSE telah diberikan kredensial akun aplikasi website BSSN VVIP program untuk melihat dan mengamati hasil dan keberlangsungan program.

14. **Menurut pengalaman Anda, bagaimana organisasi Anda menilai program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil?**

    Jawaban

    Program identifikasi kerentanan dan proteksi secara sukarela dapat dinyatakan berhasil apabila seluruh pihak dalam memahami perannya dalam program ini. Bagi kami selaku PSE, kami segera melakukan tindak lanjut perbaikan terhadap temuan kerentanan tersebut.

Tesis TomiWijaya - Magister Administrasi Publik

ORIGINALITY REPORT

19%	18%	8%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Nasional Student Paper	1%
2	peraturan.bpk.go.id Internet Source	1%
3	www.researchgate.net Internet Source	1%
4	www.jogloabang.com Internet Source	1%
5	eprints.upnyk.ac.id Internet Source	<1%
6	www.bssn.go.id Internet Source	<1%
7	repository.umsu.ac.id Internet Source	<1%
8	www.pustaka.ut.ac.id Internet Source	<1%
9	publikasi.mercubuana.ac.id Internet Source	<1%

10	jdih.bssn.go.id Internet Source	<1 %
11	Submitted to Sriwijaya University Student Paper	<1 %
12	www.slideshare.net Internet Source	<1 %
13	digilib.uin-suka.ac.id Internet Source	<1 %
14	lamongankab.go.id Internet Source	<1 %
15	nasional.kompas.com Internet Source	<1 %
16	Submitted to University of South Australia Student Paper	<1 %
17	lontar.ui.ac.id Internet Source	<1 %
18	www.scribd.com Internet Source	<1 %
19	Submitted to Forum Perpustakaan Perguruan Tinggi Indonesia Jawa Timur Student Paper	<1 %
20	www.digilib.ui.ac.id Internet Source	<1 %
21	www.kajianpustaka.com	

	Internet Source	<1 %
22	pt.scribd.com Internet Source	<1 %
23	media.neliti.com Internet Source	<1 %
24	peraturan.go.id Internet Source	<1 %
25	id.123dok.com Internet Source	<1 %
26	diskominfos.baliprov.go.id Internet Source	<1 %
27	www.smartcityindo.com Internet Source	<1 %
28	repository.unej.ac.id Internet Source	<1 %
29	Submitted to Georgia Institute of Technology Main Campus Student Paper	<1 %
30	ejournal.fisip.unjani.ac.id Internet Source	<1 %
31	netsolution.co.id Internet Source	<1 %
32	repository.untag-sby.ac.id Internet Source	

		<1 %
33	www.hukumonline.com Internet Source	<1 %
34	jurnalpost.com Internet Source	<1 %
35	Submitted to Politeknik STIA LAN Student Paper	<1 %
36	core.ac.uk Internet Source	<1 %
37	lib.lemhannas.go.id Internet Source	<1 %
38	republika.co.id Internet Source	<1 %
39	Submitted to Tarumanagara University Student Paper	<1 %
40	www.suara.com Internet Source	<1 %
41	repository.unisma.ac.id Internet Source	<1 %
42	asia.legalcentric.com Internet Source	<1 %
43	id.wikipedia.org Internet Source	<1 %

44	Submitted to University of Maryland, University College Student Paper	<1 %
45	repository.uin-suska.ac.id Internet Source	<1 %
46	jurnalprodi.idu.ac.id Internet Source	<1 %
47	Submitted to Defense University Student Paper	<1 %
48	rialvriyan.blogspot.com Internet Source	<1 %
49	Submitted to Metropolitan State University Student Paper	<1 %
50	aimos.ugm.ac.id Internet Source	<1 %
51	repository.stiegici.ac.id Internet Source	<1 %
52	sippn.menpan.go.id Internet Source	<1 %
53	Submitted to Universitas Diponegoro Student Paper	<1 %
54	mi-dnu.dp.ua Internet Source	<1 %

55	A. T. Chatfield, C. G. Reddick. "Cybersecurity Innovation in Government", Proceedings of the 18th Annual International Conference on Digital Government Research - dg.o '17, 2017 Publication	<1 %
56	journal.universitaspahlawan.ac.id Internet Source	<1 %
57	ejournal.unmus.ac.id Internet Source	<1 %
58	ppid.sumbarprov.go.id Internet Source	<1 %
59	etheses.uin-malang.ac.id Internet Source	<1 %
60	jurnalpps.uinsby.ac.id Internet Source	<1 %
61	Submitted to Universitas Indonesia Student Paper	<1 %
62	jdih.bpkp.go.id Internet Source	<1 %
63	scholar.unand.ac.id Internet Source	<1 %
64	journal.lspr.edu Internet Source	<1 %
65	bssn.go.id Internet Source	<1 %

66	repository.uinjambi.ac.id Internet Source	<1 %
67	vdocuments.site Internet Source	<1 %
68	Submitted to University of Bradford Student Paper	<1 %
69	repository.upbatam.ac.id Internet Source	<1 %
70	cris.mruni.eu Internet Source	<1 %
71	emodel.org.ua Internet Source	<1 %
72	www.antaranews.com Internet Source	<1 %
73	repository.uma.ac.id Internet Source	<1 %
74	Submitted to Dewan Perwakilan Rakyat Student Paper	<1 %
75	fliphtml5.com Internet Source	<1 %
76	jurnal.uii.ac.id Internet Source	<1 %
77	repository.ub.ac.id Internet Source	<1 %

78	uia.e-journal.id Internet Source	<1 %
79	text-id.123dok.com Internet Source	<1 %
80	docplayer.info Internet Source	<1 %
81	digilib.unila.ac.id Internet Source	<1 %
82	dspace.uii.ac.id Internet Source	<1 %
83	repositori.uma.ac.id Internet Source	<1 %
84	Submitted to Universitas Mercu Buana Student Paper	<1 %
85	binus.ac.id Internet Source	<1 %
86	e-repository.perpus.iainsalatiga.ac.id Internet Source	<1 %
87	eprints.untirta.ac.id Internet Source	<1 %
88	library.fisip-unmul.ac.id Internet Source	<1 %
89	ojs.stiami.ac.id Internet Source	<1 %

90	peraturanpedia.id Internet Source	<1 %
91	ppid.diskominfo.jatengprov.go.id Internet Source	<1 %
92	uowvivo.uow.edu.au Internet Source	<1 %
93	Submitted to Universitas Islam Indonesia Student Paper	<1 %
94	etda.libraries.psu.edu Internet Source	<1 %
95	repository.ump.ac.id Internet Source	<1 %
96	M. Roni Riswandi, Solikah Nurwati, Sanjayanto Nugroho. "Analysis of Liquidity, Firm Size, Profitability, Capital Structure and Firm Value of Oil and Gas Companies on the IDX", Jurnal Manajemen Sains dan Organisasi, 2023 Publication	<1 %
97	eprints.stiei-kayutangi-bjm.ac.id Internet Source	<1 %
98	hukum.studentjournal.ub.ac.id Internet Source	<1 %
99	id.scribd.com Internet Source	<1 %

100	ouci.dntb.gov.ua Internet Source	<1 %
101	repo.undiksha.ac.id Internet Source	<1 %
102	www.grafiati.com Internet Source	<1 %
103	www.kominfo.go.id Internet Source	<1 %
104	jdih.dprd-diy.go.id Internet Source	<1 %
105	repository.um-surabaya.ac.id Internet Source	<1 %
106	es.scribd.com Internet Source	<1 %
107	infokripto.polteksSn.ac.id Internet Source	<1 %
108	tekno.kompas.com Internet Source	<1 %
109	Submitted to ULACIT Universidad Latinoamericana de Ciencia y Tecnología Student Paper	<1 %
110	kc.umn.ac.id Internet Source	<1 %
111	nanopdf.com Internet Source	

		<1 %
112	Submitted to HTM (Haridus- ja Teadusministeerium) Student Paper	<1 %
113	Muhammad Hamad, Altaf Hussain, Majida Khan Tareen. "chapter 7 Data Leakage and Privacy Concerns in Public Bug Bounty Platforms", IGI Global, 2023 Publication	<1 %
114	Submitted to Universiti Teknologi Petronas Student Paper	<1 %
115	disdik.jambiprov.go.id Internet Source	<1 %
116	ejournal.sisfokomtek.org Internet Source	<1 %
117	eprints.uns.ac.id Internet Source	<1 %
118	haibanten.co.id Internet Source	<1 %
119	repository.unhas.ac.id Internet Source	<1 %
120	aptika.kominfo.go.id Internet Source	<1 %
	www.math.ui.ac.id	

121	Internet Source	<1%
122	Submitted to Ajou University Graduate School Student Paper	<1%
123	Submitted to IAIN Syaikh Abdurrahman Siddik Bangka Belitung Student Paper	<1%
124	Kholilah Samosir, Hendra Dhermawan Sitanggang. "PEMICUAN JAMBAN SEHAT SEBAGAI SOLUSI BEBAS BUANG AIR BESAR SEMBARANGAN PADA MASYARAKAT KAMPUNG BULANG KOTA TANJUNGPINANG", Jurnal Salam Sehat Masyarakat (JSSM), 2020 Publication	<1%
125	digilib.uinsby.ac.id Internet Source	<1%
126	www.peraturan.go.id Internet Source	<1%
127	Meriska Yosiana, Ratna Wulandari. "KOMODIFIKASI TUBUH PEREMPUAN PADA TARIAN JOGED BUMBUNG BALI DI YOUTUBE", Jurnal Ilmiah Multidisiplin, 2023 Publication	<1%
128	Submitted to Unika Soegijapranata Student Paper	<1%
129	Submitted to University of Warwick	

	Student Paper	<1 %
130	educalingo.com Internet Source	<1 %
131	ejournal.universitasmahendradatta.ac.id Internet Source	<1 %
132	lpgr.fisip.uns.ac.id Internet Source	<1 %
133	radentaufiq.wordpress.com Internet Source	<1 %
134	Submitted to Politeknik Negeri Jakarta Student Paper	<1 %
135	adoc.pub Internet Source	<1 %
136	dutatv.com Internet Source	<1 %
137	ejurnal.ubharajaya.ac.id Internet Source	<1 %
138	jdihkepri.kemenkumham.go.id Internet Source	<1 %
139	ris.utwente.nl Internet Source	<1 %
140	Submitted to Clarkston Community Schools Student Paper	<1 %

141	Submitted to Exeed College Student Paper	<1 %
142	Submitted to UT, Dallas Student Paper	<1 %
143	Vella Nur Cahya Ningtyas, Ria Angin. "Inovasi Menuju Transformasi Digital dalam Pelayanan Publik Kajian Sistem Manajemen Pelayanan Desa (SIMPEDA) di Desa Balung Lor", Indonesian Journal of Public Administration Review, 2023 Publication	<1 %
144	eprints.unm.ac.id Internet Source	<1 %
145	journal.stkipsubang.ac.id Internet Source	<1 %
146	jurnal.kominfo.go.id Internet Source	<1 %
147	kwbcjatengdiy.beacukai.go.id Internet Source	<1 %
148	ppid.sulbar.bawaslu.go.id Internet Source	<1 %
149	teknologi.bisnis.com Internet Source	<1 %
150	vdocuments.pub Internet Source	<1 %

151	www.umko.ac.id Internet Source	<1 %
152	Submitted to Universitas Brawijaya Student Paper	<1 %
153	Submitted to Universitas Pamulang Student Paper	<1 %
154	diskominfo.kendalkab.go.id Internet Source	<1 %
155	ibtpi.pelitaindonesia.ac.id Internet Source	<1 %
156	jurnalkonstitusi.mkri.id Internet Source	<1 %
157	Submitted to Landmark University Student Paper	<1 %
158	Submitted to Technological University Dublin Student Paper	<1 %
159	Submitted to Universitas Negeri Jakarta Student Paper	<1 %
160	Submitted to Universitas Pakuan Student Paper	<1 %
161	Submitted to University of Northumbria at Newcastle Student Paper	<1 %
162	cakrawalajournal.org Internet Source	

		<1 %
163	issuu.com Internet Source	<1 %
164	journals.iupui.edu Internet Source	<1 %
165	kompaspedia.kompas.id Internet Source	<1 %
166	panwaslutasikmalayakab.wordpress.com Internet Source	<1 %
167	ppid.lan.go.id Internet Source	<1 %
168	repository.iainpare.ac.id Internet Source	<1 %
169	www.eccouncil.org Internet Source	<1 %
170	www.scilit.net Internet Source	<1 %
171	fankychristian.blogspot.com Internet Source	<1 %
172	fkmhii.com Internet Source	<1 %
173	Submitted to Grand Canyon University Student Paper	<1 %

174	Listyawati, Peni Rinda. "Rekonstruksi Regulasi Corporate Social Responsibility Berbasis Asas Ta'Awun", Universitas Islam Sultan Agung (Indonesia), 2023 Publication	<1 %
175	Ringgo Saprianto, Tiur Roida Simbolon, Alexandra Hukom. "Implikasi Otonomi Daerah Pada Pembangunan Sektor Pendidikan dan Kesehatan di Indonesia", JEPP : Jurnal Ekonomi Pembangunan Dan Pariwisata, 2023 Publication	<1 %
176	Submitted to Universitas 17 Agustus 1945 Semarang Student Paper	<1 %
177	doaj.org Internet Source	<1 %
178	etheses.bham.ac.uk Internet Source	<1 %
179	islamicmarkets.com Internet Source	<1 %
180	koran.tempo.co Internet Source	<1 %
181	repository.helvetia.ac.id Internet Source	<1 %
	www.domainesia.com	

182	Internet Source	<1%
183	Submitted to Fakultas Ekonomi Universitas Indonesia Student Paper	<1%
184	Submitted to Police Academy – University of Police Science Student Paper	<1%
185	Submitted to Universitas Muhammadiyah Ponorogo Student Paper	<1%
186	Submitted to Universitas Mulawarman Student Paper	<1%
187	jurnal.ipb.ac.id Internet Source	<1%
188	jurnal.poltekapp.ac.id Internet Source	<1%
189	jurnal.um-tapsel.ac.id Internet Source	<1%
190	jurnalmahasiswa.unesa.ac.id Internet Source	<1%
191	Submitted to poltekim Student Paper	<1%
192	repository.unja.ac.id Internet Source	<1%

193	www.bpkp.go.id Internet Source	<1 %
194	www.idxchannel.com Internet Source	<1 %
195	Submitted to UM Surabaya Student Paper	<1 %
196	Submitted to Universitas Negeri Semarang Student Paper	<1 %
197	password-generator.soft143.com Internet Source	<1 %
198	www.eprints.unram.ac.id Internet Source	<1 %
199	Muhammad Reza Ramdani, Andi Muara Arumbarkah, Ismi Ayu Lestari. "The Perception of Auditor Career From University Students Perspective", JEMA: Jurnal Ilmiah Bidang Akuntansi dan Manajemen, 2019 Publication	<1 %
200	goodstats.id Internet Source	<1 %
201	repository.uinjkt.ac.id Internet Source	<1 %
202	repository.unsri.ac.id Internet Source	<1 %

203	sefidvash.net Internet Source	<1 %
204	www.medcom.id Internet Source	<1 %
205	"ICT Systems Security and Privacy Protection", Springer Science and Business Media LLC, 2020 Publication	<1 %
206	Submitted to Universitas Amikom Student Paper	<1 %
207	Widya Prameswari Pertiwi, Imam Muhtarom, Dewi Herlina Sugiarti. "Perjuangan Hidup Tokoh Utama Novel 23 Episentrum Karya Adenita dan Relevansinya terhadap Materi Ajar Sastra di SMA Tinjauan Sosiologi Sastra", Silampari Bisa: Jurnal Penelitian Pendidikan Bahasa Indonesia, Daerah, dan Asing, 2021 Publication	<1 %
208	eprints.ums.ac.id Internet Source	<1 %
209	etheses.iainponorogo.ac.id Internet Source	<1 %
210	idoc.pub Internet Source	<1 %
211	jdih.maritim.go.id Internet Source	<1 %

212	pdffox.com Internet Source	<1 %
213	repositori.usu.ac.id Internet Source	<1 %
214	repository.ar-raniry.ac.id Internet Source	<1 %
215	repository.undwi.ac.id Internet Source	<1 %
216	repository.unik-kediri.ac.id Internet Source	<1 %
217	skripsi-ilmiah.blogspot.com Internet Source	<1 %
218	spbe.go.id Internet Source	<1 %
219	vk9-sec.com Internet Source	<1 %
220	www.bkn.go.id Internet Source	<1 %
221	Pedersen, Dane. "Trust, Control, and Risk in the Salish Sea: A Case Study of the Transboundary Network Governing the Endangered Southern Resident Killer Whale", McGill University (Canada), 2023 Publication	<1 %

222	Ping Chen, Jonas Visschers, Cedric Verstraete, Letizia Paoli, Christophe Huygens, Lieven Desmet, Wouter Joosen. "The relationship between the cost of cybercrime and web security posture", Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, 2017 Publication	<1 %
223	Submitted to School of Business and Management ITB Student Paper	<1 %
224	bdlhkkupang.bp2sdm.menlhk.go.id Internet Source	<1 %
225	e-journals.unmul.ac.id Internet Source	<1 %
226	ejournal.umm.ac.id Internet Source	<1 %
227	elsam.or.id Internet Source	<1 %
228	eprints.uny.ac.id Internet Source	<1 %
229	estd.perpus.untad.ac.id Internet Source	<1 %
230	hadi-shop.blogspot.com Internet Source	<1 %

231	j-ilkominfo.org Internet Source	<1 %
232	journal.ipm2kpe.or.id Internet Source	<1 %
233	jurnal.ikbis.ac.id Internet Source	<1 %
234	mafiadoc.com Internet Source	<1 %
235	monitortangerang.com Internet Source	<1 %
236	nesia.ir Internet Source	<1 %
237	ngopilu.blogspot.com Internet Source	<1 %
238	policyreview.info Internet Source	<1 %
239	repository.nusaputra.ac.id Internet Source	<1 %
240	repository.unwira.ac.id Internet Source	<1 %
241	sinta.unud.ac.id Internet Source	<1 %
242	www.bca.co.id Internet Source	<1 %

243	www.infosoloraya.com Internet Source	<1%
244	www.sidogiri.net Internet Source	<1%
245	123dok.com Internet Source	<1%
246	Dwi Indriastuti, Mia Priluddina, Ryan Budi Rusmana, Toni Yuliyanto. "Tata Kelola Kolaboratif Program Ketahanan Pangan di Kodim 0733 Kota Semarang", Al Qalam: Jurnal Ilmiah Keagamaan dan Kemasyarakatan, 2023 Publication	<1%
247	Rohmaniah, Sanivatun. "Kekuatan Pembuktian Akta Notaris Yang Dibuat Secara Elektronik Dalam Sistem Hukum Indonesia", Universitas Islam Sultan Agung (Indonesia), 2023 Publication	<1%
248	Vaishali Hegde. "Cybersecurity for Medical Devices", 2018 Annual Reliability and Maintainability Symposium (RAMS), 2018 Publication	<1%
249	acch.kpk.go.id Internet Source	<1%
250	addiniurwah.blogspot.com Internet Source	<1%

251	anri.go.id Internet Source	<1 %
252	arifudinfahmi.blogspot.com Internet Source	<1 %
253	codeigniter.com Internet Source	<1 %
254	digilib.iain-palangkaraya.ac.id Internet Source	<1 %
255	digilib.uns.ac.id Internet Source	<1 %
256	digilibadmin.unismuh.ac.id Internet Source	<1 %
257	ilmuhukum29.blogspot.com Internet Source	<1 %
258	imamroyani.blogspot.com Internet Source	<1 %
259	journal.sinov.id Internet Source	<1 %
260	journal.uinsgd.ac.id Internet Source	<1 %
261	journal.umy.ac.id Internet Source	<1 %
262	jurnal.stts.edu Internet Source	<1 %

263	jurnal.ugm.ac.id Internet Source	<1 %
264	jurnal.usu.ac.id Internet Source	<1 %
265	lib.ibs.ac.id Internet Source	<1 %
266	lib.ui.ac.id Internet Source	<1 %
267	library.unismuh.ac.id Internet Source	<1 %
268	mbscenter.or.id Internet Source	<1 %
269	mochamadimronrux.blogspot.com Internet Source	<1 %
270	pandeglangkab.bawaslu.go.id Internet Source	<1 %
271	repo.usni.ac.id Internet Source	<1 %
272	repositori.uin-alauddin.ac.id Internet Source	<1 %
273	repository.fisip-untirta.ac.id Internet Source	<1 %
274	repository.policy.paramadina.ac.id Internet Source	<1 %

275	repository.unair.ac.id Internet Source	<1 %
276	repository.unj.ac.id Internet Source	<1 %
277	repository.uph.edu Internet Source	<1 %
278	repository.widyatama.ac.id Internet Source	<1 %
279	sodiqpks.blogspot.com Internet Source	<1 %
280	worldwidescience.org Internet Source	<1 %
281	www.coursehero.com Internet Source	<1 %
282	www.econstor.eu Internet Source	<1 %
283	www.idntimes.com Internet Source	<1 %
284	www.jurnal-umbuton.ac.id Internet Source	<1 %
285	www.kompasiana.com Internet Source	<1 %
286	www.neliti.com Internet Source	<1 %

287	www.saplaw.top Internet Source	<1%
288	zombiedoc.com Internet Source	<1%
289	Bambang Ari Satria, Hermianto Hermianto. "Collaborative Governance Dalam Program Perhutanan Sosial Pada HKm Gempa 01 Kurau Barat Bangka Belitung", Jurnal Ilmu Administrasi Negara (JUAN), 2020 Publication	<1%
290	Lestariani Telaumbanua, Ayler Beniah Ndraha, Yupiter Mendrofa, Sukaaro Waruwu. "KOLABORASI ORGANISASI DALAM MENGIMPLEMENTASIKAN PROGRAM KELUARGA HARAPAN (PKH) DI DESA SISARAHILIGAMO KECAMATAN GUNUNGSTOLI KOTA GUNUNGSITOLI", JMBI UNSRAT (Jurnal Ilmiah Manajemen Bisnis dan Inovasi Universitas Sam Ratulangi)., 2023 Publication	<1%
291	Maslia Qomar, Zulkifli Muhadli. "Pemanfaatan Media Digital Pada Sistem Pemerintahan: Studi Literatur Berbantuan Nvivo 12 Pro", Jurnal Humanitas: Katalisator Perubahan dan Inovator Pendidikan, 2023 Publication	<1%

292	Pusparukmi, Nirwanadewi. "Perlindungan Hukum Bagi Pemilik Sertipikat Tanah Yang Titik Koordinatnya Berbeda Dengan Objek Tanah", Universitas Islam Sultan Agung (Indonesia), 2023 Publication	<1 %
293	Putri Herlinia Erika, Septi Wulandari, Musta'ana Musta'ana. "Collaborative Governance Dalam Pencegahan Pernikahan Usia Anak Di Kabupaten Bojonegoro", Sawala : Jurnal Administrasi Negara, 2023 Publication	<1 %
294	asepsulaemantea.wordpress.com Internet Source	<1 %
295	eprints.itn.ac.id Internet Source	<1 %
296	repository.uki.ac.id Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		