Vol. 3, No. 4, Desember 2024
e-ISSN: 2964-1322
p-ISSN: 2964-9595

JIPOSSTER: Jurnal Ilmu Politik dan Studi Sosial Terapan

Keamanan Sistem Informasi Pemilu Melalui *Computer Security Incident Response Team (Csirt)* Pemilu Serentak 2024

Ricky Febriansyah [(1)*] Ana Husnayanti [(1)]
[(1)]KPU Kabupaten Bangka Tengah, Koba, Indonesia
[(2)] Poltekkes Kemenkes Pangkalpinang, Pangkalpinang, Indonesia
Email : [(a*)] ricky.febriansyah290284@gmail.com

ABSTRAK

Komisi Pemilihan Umum bersama Badan Siber dan Sandi Negara (BSSN) membentuk Computer Security Incident Response Team (CSIRT) atau Tim Tanggap Keamanan Insiden Siber untuk mengamankan sistem informasi pendukung pemilihan umum dari kejahatan siber. Dengan pendekatan analisis Strength, Weakness, Opportunities, Threats (SWOT) , kajian ini bertujuan untuk mengetahui :1). Penyebab sistem informasi sering diserang; 2).kendala pencegahan kejahatan sistem informasi pemilu; 3). Akibat serangan siber yang tidak terbendung; 4). Solusi penerapan KPU-CSIRT; 5). Potensi permasalahan penerapan KPU-CSIRT; dan 6). Strategi pelaksanaan CSIRT. Penelitian ini menggunakan pendekatan kualitatif dengan metode pengumpulan data melalui observasi dan studi dokumen. Hasil penelitian sistem informasi pemilu sering diserang disebabkan oleh masih lemahnya keamanan siber KPU dan faktor manusia. penerapan CSIRT menghadapi beberapa potensi seperti Sumber Daya Manusia, anggaran dan infrastruktur, ancaman berita hoax pemilu dan pemilihan terutama output sistem informasi yang diterapkan, penerapan Peraturan Komisi Pemilihan Umum Nomor 5 tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik dapat menjadi acuan dalam penerapan CSIRT.

Kata kunci: Sistem Informasi, Keamanan Pemilu, Pemilu dan Pemilihan Serentak

ABSTRACT

The General Elections Commission together with the National Cyber and Crypto Agency (BSSN) formed a Computer Security Incident Response Team (CSIRT) to secure information systems supporting elections from cybercrimes. With a SWOT (Strength, Weakness, Opportunities, Threats) analysis approach, this study aims to determine: 1). Causes of information systems are often attacked; 2). obstacles to preventing election information system crimes; 3). As a result of unstoppable cyber attacks; 4). KPU-CSIRT implementation solutions; 5). Potential problems with the implementation of KPU-CSIRT; and 6). CSIRT implementation strategy. This study uses a qualitative approach with data collection methods through observation and document study. The results of research on election information systems are often attacked due to the weakness of KPU cyber security and human factors. the implementation of CSIRT faces several potentials such as human resources, budget and infrastructure, the threat of election and election hoax news, especially the information system output that is applied, the implementation of the General Election Commission Regulation Number 5 of 2021 concerning the Implementation of an Electronic-Based Government System can be a reference in the implementation of CSIRT.

Keywords: *Information Systems, Election Security, Elections and Simultaneous Elections*

Submit:	Revised:	Accepted:	Available online:
20.10.2024	09.11.2024	07.12.2024	31.12.2024

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

PENDAHULUAN

Masyarakat digital dan sistem pemerintahan digital telah mengubah kegiatan dan aktivitas secara konvensional menjadi digital. Dengan transformasi digital ini membantu dalam proses pengelolaan digital sehingga mempermudah masyarakat dalam memperoleh informasi. Akan tetapi pada proses dan kemudahan memperoleh informasi terdapat ancaman serangan siber.ugas pemerintah dan dukungan masyarakat dalam menghadapi serangan siber harus cepat ditindaklanjuti. Serangan siber keamanan sistem informasi digital akan menimbulkan kerugian finansial, fisik bahkan mengancam stabilitas nasional.

Maraknya serangan siber di Indonesia berpotensi terjadinya insiden pada perusahaan maupun instansi. Menurut data yang dikeluarkan oleh Badan Siber Sandi Negara (BSSN) terdapat 290,3 juta kasus serangan siber pada tahun 2019. Jika melihat pada tahun 2018 yang lalu dengan total 232, 4 juta kasus (Anjani, 2021). Tentu dengan penambahan kasus yang cukup signifikan terlebih pada masa sekarang pandemi covid-19 dimana masyarakat terjadi perubahan perilaku dalam kegiatan sehari-hari terjadinya percepatan transformasi digital Indonesia. Berdasarkan data dari Kementerian Komunikasi dan Informatika (kominfo) menyebutkan bahwa pengguna internet di Indonesia mencapai 202,6 juta pengguna pada tahun 2021, kemudian mengalami kenaikan sebesar 175,4 juta pengguna pada tahun 2022. (Agustini, 2021)

Demi menghadapi dan mengamankan sistem informasi dari serangan siber. Komisi Pemilihan Umum (KPU) berkolaborasi dengan BSSN membentuk KPU-CSIRT (Computer Security Incident Response Team) atau Tim Tanggap Keamanan Insiden Siber untuk mengamankan sistem informasi pendukung pemilihan umum dari kejahatan siber. Pembentukan tim ini telah dilaksanakan pada hari Jum'at, 21 Januari 2022. Sebagai kesiapan KPU dalam menghadapi pemilu serentak 2024 dari ancaman serangan siber seperti berita hoax, kebocoran data dan administrasi pemilu. Berbagai kegiatan yang akan dilakukan melalui peningkatan Sumber Daya Manusia (SDM) melalui pelatihan, workshop dan cyber security drill atau simulasi penanganan bencana di dunia maya. KPU-CSIRT mendapat dukungan dari CSIRT Nasional melalui Deputi Bidang Operasi Keamanan Siber dan Sandi BSSN melalui layanan reaktif dalam bentuk koordinasi insiden, trase insiden, dan resolusi insiden.(BSSN, 2022)

Penerapan CSIRT merupakan proyek prioritas (Major Project) seperti yang dituangkan dalam Peraturan Presiden Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020 – 2024. BSSN diamanatkan untuk membentuk CSIRT sektor pemerintah sebanyak 131 CSIRT yang dilaksanakan selama 5 (lima) tahun. Rencana kerja pemerintah membentuk 131 CSIRT terdiri 87 Kementerian/Lembaga dan 34 Pemerintah Provinsi. Pada tahun 2020 telah terbentuk sebanyak 15 Kementerian/Lembaga dan Pemerintahan Provinsi, selanjutnya tahun 2021 telah terbentuk sebanyak 39 Kementerian/Lembaga dan Pemerintahan Provinsi. KPU termasuk Instansi pusat yang mendapatkan bagian pembentukan CSIRT pada tahun 2022 ini bersama 32 Kementerian Pusat dan Daerah lainnya. Pada tahun 2023 akan dibentuk sebanyak 36 CSIRT Kementerian Lembaga Daerah, terakhir rencana tahun 2024 akan dibentuk 10 Kementerian/Lembaga dan Daerah CSIRT.

Penyelenggaraan pemilu dan pemilihan tidak luput dari serangan siber karena dalam pelaksanaannya KPU menggunakan kemajuan teknologi informasi dalam penyelenggaraan pemilu dan pemilihan baik di tingkat pusat, daerah dan badan adhoc. KPU memiliki beberapa sistem informasi dalam penyelenggaraan pemilu dan pemilihan, seperti Sistem Informasi Data Pemilih (Sidalih), Sistem Informasi Partai Politik (Sipol), Sistem Informasi Pencalonan (Silon), Sistem Informasi Daerah Pemilih (Sidapil), Sistem Informasi Penghitungan (Situng) dan menggunakan Sistem Informasi Rekapitulasi Elektronik (Sirekap) untuk pemilihan tahun 2020. Sistem Informasi yang digunakan KPU mendapatkan serangan siber seperti situng yang menampilkan data hasil hitung cepat pada pemilihan serentak 2018 di 171 daerah pada hari pemungutan suara, sipol pada pemilu 2019 mengalami kemacetan sistem, tidak bisa diakses, dan terjadinya migrasi data, sidalih yang menyimpan lebih dari 190 juta data pemilih tidak

dapat menghapus data ganda secara optimal karena kesulitan operator daerah dalam mengakses sidalih. Peristiwa peretasan terjadi ketika adanya laporan dari Cyber Crime Kepolisian Republik Indonesia perihal peretasan situng yang dilakukan oleh seorang anak berusia 14 tahun (Pratama dan Amalia, 2019: 100). Berdasarkan beberapa kasus sering terjadinya serangan siber yang mengganggu keamanan siber sistem informasi. KPU sendiri sudah melakukan audit sistem akan tetapi ketika terjadinya insiden siber pemilu yang melanda, KPU memerlukan tim yang tanggap dalam menghadapi insiden terjadinya serangan siber yaitu melalui KPU-CSIRT.

Berbagai kasus keamanan sistem pemilu yang terjadi pada pemilu dan pemilihan memerlukan suatu tindakan yaitu pembentukan KPU-CSIRT. Diharapkan dengan adanya pembentukan KPU-CSIRT dapat mengamankan sistem informasi milik KPU terutama dalam penyelenggaraan tahapan pemilu 2024 nanti. KPU-CSIRT juga dapat menjawab berbagai respon dari KPU Daerah yang menyelenggarakan berbagai tahapan pemilu di tingkat daerah. Kabupaten Bangka Tengah merupakan daerah yang telah menyelenggarakan periode pemilu dan pemilihan yang berdekatan. Beberapa penyelenggaraan pemilu dan pemilihan 2014-2020 seperti pemilu 2014 dan 2019, pemilihan Bupati dan Wakil Bupati Bangka Tengah tahun 2015 dan 2020, pemilihan Gubernur dan Wakil Gubernur Kepulauan Bangka Belitung tahun 2017. Dampaknya pada penghelatan yang terjadi isu-isu nasional terjadi di Kabupaten Bangka Tengah terlebih persiapan tahapan pemilu serentak 2024 nanti. Selain KPU-CSIRT memerlukan respon dari KPU Daerah, KPU Kabupaten Bangka Tengah memiliki SDM yang kompeten dalam penerapan sistem informasi pemilu. Berdasarkan permasalahan diatas, tulisan ini membahas tentang bagaimana tantangan dalam penerapan CSIRT menghadapi pemilu serentak 2024 dari ancaman serangan siber dan juga perlu adanya respon dari KPU Daerah dalam hal ini KPU Kabupaten Bangka Tengah.

Penerapan teknologi informasi dalam Pemilu di Indonesia bertujuan untuk mempermudah kerja penyelenggara pemilu dan meningkatkan kepercayaan pemilih dan peserta pemilih terhadap proses pemilu. KPU memiliki 3 (tiga) kategori dalam penerapan teknologi informasi yaitu 1).Persiapan pemilu; 2). Pelaksanaan pemilu dan 3). Pasca pelaksanaan pemilu. Berdasarkan pengalaman pemilu dan pemilihan, penerapan Teknologi Informasi telah memberikan kontribusi, seperti sistem informasi data pemilih (sidalih) berfungsi sebagai tabulasi terhadap daftar nama-nama warganegara yang sudah memiliki hak pilih untuk mendorong akurasi daftar pemilih. Sistem informasi selanjutnya adalah Sistem Informasi Partai Politik (sipol), sistem informasi ini memiliki perangkat daring untuk mempermudah tahapan pendaftaran dan verifikasi partai politik. KPU mengembangkan Sistem Informasi Pencalonan (silon) pada pemilihan 2015 dan diperuntukan proses pendaftaran calon kepala daerah pada pemilihan. Untuk mengontrol pendistribusian logistik, KPU mengembangkan sistem informasi logistik (silog), dalam hal dana kampanye, KPU mengembangkan sistem informasi data kampanye (sidarkam). Sistem informasi yang dikembangkan oleh KPU merupakan suatu usaha independensi dan meningkatkan kepercayaan publik pada proses dan hasil pemilu yang transparan dan akuntabilitas data pemilu.(Pratama dan Salabi, 2019).

KPU-CSIRT yang dibentuk untuk mengamankan sistem informasi KPU dalam menyelenggarakan tahapan pemilu dan pemilihan terutama pada pemilu 2024 nanti. Untuk itu hal yang harus menjadi perhatian adalah Cyber Security atau keamanan siber. Cyber security bertujuan untuk melindungi informasi baik secara physical attack maupun *cyber attack*, elemen terdiri dari dokumen security policy, informasi infrastruktur perimeter defense, *network monitoring, system information* dan event manajemen dan *network security assessment*. (Ardiyanti, 2014:99). Keamanan siber merupakan kumpulan alat,kebijakan, konsep keamanan perlindungan keamanan, pedoman, pendekatan, manajemen resiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi, Tujuannya melindungi lingkungan dan organisasi siber serta aset pengguna Keamanan Sistem Informasi Pemilu, setidaknya ada 3 tujuan umum keamanan siber menurut The Estonian Information System Authority (RIA) yaitu kerahasiaan, integritas dan ketersediaan.(European Commission, 2018:7)

Berbagai negara yang menggunakan teknologi Informasi termasuk Indonesia yang menggunakan beberapa sistem informasi dalam pemilu perlu memastikan sistem keamanan dari serangan siber. Pada penyelenggaraan pemilihan 2020, KPU telah menerapkan sistem informasi rekapitulasi (Sirekap). Ada beberapa hal yang harus dilakukan KPU untuk mengamankan KPU yaitu :1),Kecukupan Tenaga Teknologi Informasi (IT) ; 2). Kontrol terhadap petugas; 3).Kategoris Data; 4). Back Up Data; 5). Mendapatkan Sertifikat ISO 27001; 6). Uji coba Audit; 7). Sosialisasi dan edukasi keamanan siber; dan 8). Membentuk satuan tugas (rumahpemilu.org). Pada prinsip point 8 membentuk gugus tugas jika kejadian peretasan tentu dapat diterapkan CSIRT atau Computer Security Incident Response Team.

Istilah penerapan CSIRT atau CERT (Computer Emergency Response Team) di dunia telah dilakukan dan memiliki beberapa nama seperti Computer Emergency Response Team/Coordination Center (CERT/ICC), Computer Incident Response Team (CIRT), Incident Response Team (IRT), Security Emergency Team (SERT), dan Warning Advice and Reporting Point (WARP's) (Maria, etc, 2014). Manajemen siber insiden merupakan rangkaian proses sekuensial yang terdiri dari fase persiapan, fase deteksi insiden, fase penanganan, fase mitigasi, fase pemilihan dan fase pembelajaran dari insiden yang terjadi. Manajemen insiden ini merupakan langkah proaktif dalam menyelesaikan suatu insiden, dengan menggunakan model SIM3 dan CREST adalah dua kerangka kerja utama dalam manajemen insiden. (Hendra & Hanita, 2020)

CSIRT merupakan organisasi atau tim yang bertanggung jawab untuk menerima, meninjau dan menanggapi laporan dan aktivitas insiden keamanan siber. Fungsi CSIRT Membuka layanan reaktif terdiri koordinasi insiden, triase insiden dan realisasi insiden, memberikan layanan posesif, mempublikasi informasi kerawanan dan tren teknologi dan auto keamanan informasi, memberikan layanan peningkatan kualitas keamanan bersifat konsultasi, cyber drill pelatihan dan workshop.

Serangan secara teknis, serangan siber sering terjadi pada sistem registrasi data pemilih online, sistem teknologi pungut-hitung, sistem transmisi hasil, teknologi agregasi data, situs web untuk mempublikasi hasil, situs layanan pemilihan online, akun email institusi dan pribadi penyelenggara pemilu dan sistem komunikasi penyelenggara pemilu. Dari berbagai serangan tersebut, serangan berupa Denial-of-Service (DoS) yang mengakibatkan sistem overload atau kelebihan beban sehingga kerja sistem menjadi lambat. Serangan ini sering terjadi pada sistem transmisi hasil KPU Ukraina pada pemilu presiden dan legislatif 2014. (Ellena et al., 2018).

Kerangka Kerja (Nist, 2018), kerangka kerja merupakan pendekatan berbasis risiko untuk pengelolaan risiko keamanan siber dan terdiri dari inti kerangka kerja, level pelaksana kerangka kerja dan profil kerangka kerja. Dalam hal pengamanan siber penyelenggaraan sistem elektronik melalui penerapan sertifikat SNI 27001 sistem keamanan informasi sangat penting karena menyangkut informasi yang digunakan. Dalam standar penerapan persyaratan perlu penetapan, penerapan, pengoperasiaan, pemantauan, pengkajian, peningkatan dan pemeliharaan sistem manajemen keamanan informasi (SMKI) yang terdokumentasi dalam konteks resiko bisnis keseluruhan (Setiawan, 2015). Beberapa tahapan pengembangan CSIRT menurut versi Carnegie Mellon University) (CMU SEI) terdiri dari tahapan pendidikan dan pembinaan, tahapan perencanaan, tahapan implementasi, operasional CSIRT, dan kolaborasi (Setiawan, 2013). Sistem Keamanan secara umum meliputi confidentiality, integrity, dan availability (CIA) merupakan aturan turunan dasar dari keamanan jaringan atau informasi (Hayaty, 2020).

KPU telah menetapkan PKPU Nomor 5 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan umum yang memiliki tujuan untuk meningkatkan keterpaduan dan efisien sistem pemerintahan berbasis elektronik dan mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya di KPU, KPU Provinsi dan KPU Kabupaten/kota. (Bouty et al., 2019) penilaian SPBE di Pemerintahan Kota Gorontalo menunjukan hasil yang baik. Pelaksanaan Sistem Pemerintahan Berbasis Elektronik (SPBE) memiliki tujuan untuk mewujudkan proses pemerintahan yang lebih efektif, efisien, transparan dan akuntabel dalam

pelayanan publik di Kabupaten Sumbawa dimana evaluasi SPBE menunjukan hasil yang memuaskan (Pratiwi et al., 2020).

Sistem Manajemen Keamanan Informasi (SMKI) di Fakultas Teknik Universitas Ibn Khaldun (UIKA) Bogor berdasarkan ISO/ICE 27001:2013 berdasarkan hasil pembahasan kurang aman menurut standar karena tingkat keamanan sebesar 49% dan pihak manajemen hanya mempersaia tingkat keamanan sebesar 45% (Goeritno & Hendrawan, 2016). KPU telah mengeluarkan Surat Edaran Nomor 3 tahun 2022 tentang Penerapan Kebijakan Sistem Manajemen Keamanan Informasi. Cara pencegahan serangan peretasan dalam penerapan kebijakan sistem manajemen keamanan sistem informasi (SMKI) berdasarkan standar ISO/IEC 27001:2013, dimana terdapat 29 poin pencegahan peretasan yang wajib diterapkan oleh KPU, KPU/KIP Provinsi dan KPU/KIP Kabupaten/kota. Dalam rutinitas pekerjaan, KPU memiliki berbagai macam aplikasi baik itu khusus untuk kepemiluan ataupun non kepemiluan seperti SIMONIKA. KPU telah melakukan sosialisasi terkait Surat edaran nomor 3 tahun 2022 ini kepada KPU Provinsi dan KPU Kabupaten/Kota, termasuk KPU Kabupaten Bangka Tengah, pada hari Selasa, 22 Februari 2022 secara daring.

Berdasarkan permasalahan di atas dan beberapa penelitian terdahulu, maka penelitian ini bertujuan untuk 1). Mengapa sistem informasi kerap terjadi serangan siber pada pemilu; 2). Apa kendala-kendala yang dihadapi dalam mencegah dan mengatasi kejahatan siber pada pemilu dan pemilihan terdahulu; 3). Apa saja akibat yang terjadi ketika kejahatan serangan siber terhadap sistem informasi yang tidak terbendung; 4). Apa Solusi agar pelaksanaan Computer Security Incident Response Team (CSIRT) untuk mengamankan sistem informasi pendukung pemilu dari kejahatan terlebih optimal pada pemilu serentak 2024 nanti; 5). Potensi masalah yang bakal dihadapi oleh pelaksanaan CSIRT untuk mengamankan sistem informasi pendukung pemilu dari kejahatan siber; dan 6). Apa strategi agar pelaksanaan CSIRT untuk mengamankan sistem informasi pendukung pemilu dari kejahatan siber bisa efektif penggunaanya pada pemilu serentak 2024.

Penelitian ini menggunakan pendekatan analisis SWOT (Strength, Weakness, Opportunities, Threats). Analisis ini didasarkan pada logika yang dapat memaksimalkan kekuatan (strength) dan peluang (opportunities), namun secara bersamaan dapat meminimalkan kelemahan (weakness) dan ancaman (threats).(Astuti & Ratnawati, 2020)

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian studi pustaka atau riset pustaka. Menurut Zed (2014) Riset Pustaka (*library research*) adalah penelusuran pustaka tidak hanya untuk langka mempersiapkan secara awal kerangka penelitian (*research design*) akan tetapi memanfaatkan sumber-sumber perpustakaan memperoleh data penelitian. Pada penelitian ini menggunakan metode pengumpulan data dengan mengambil data di pustaka, membaca dan menggali bahan penelitian dari beberapa jurnal, karya ilmiah, buku dan berita serta informasi dari media cetak dan online sebagai informasi serta melakukan observasi. Meliputi data berupa CSIRT dan Keamanan Sistem Informasi Pemilu dan data pemilu 2019 dan pemilihan 2020 serta persiapan 2024.

Dalam penelitian studi pustaka, terdapat ciri utama yaitu 1). Peneliti berhadapan langsung dari teks, data, angka bukan dengan pengetahuan langsung dari lapangan; 2). Data pustaka bersifat “siap pakai” artinya peneliti tidak terjung langsung ke lapangan karena peneliti berhadapan langsung dengan sumber data; 3). Bersumber dari tangan kedua bukan dari orisinil di tangan pertama di lapangan; dan 4). Kondisi data pustaka tidak dibatasi ruang dan waktu, maka peneliti menggunakan dengan cara penelaahan kemudian mengeksplorasi sumber yang berasal dari jurnal, buku dan dokumen cetak dan elektronik serta sumber-sumber informasi yang mengandung data dan dianggap relevan dengan penelitian.

HASIL DAN PEMBAHASAN

Penyebab Sistem Informasi Kerap Terjadi Serangan Siber Pada Pemilu

Berbagai sistem informasi yang telah dikembangkan oleh KPU dalam menunjang tahapan pemilu dan pemilihan. (Kurnia dan Manahan, 2019, 262:278) yaitu :1)Sistem informasi partai politik (Sipol) yang didesain untuk memberikan pelayanan kepada partai politik untuk mengisi data kepengurusan dan anggota dan membantu KPU melakukan verifikasi administrasi dan faktual; 2). Sistem Informasi Data Pemilih (Sidalih), merupakan sebuah aplikasi yang digunakan oleh KPU untuk menyusun dan pemutakhiran daftar pemilih untuk kebutuhan penyelenggaraan pemilu di Indonesia; 3).Sistem Informasi Penghitungan Suara (Situng) sebagai sarana KPU dalam membuat arsip digital hasil pemilu berupa formulir C1, formulir DAA, DA1, DB1 dan DC1 serta sebagai sarana mempublikasikan hasil pemilu dalam bentuk image maupun excel; 4).Sistem Informasi Pencalonan (Silon), terdapat 2 versi yaitu versi pertama pada pemilihan 2015, aplikasi berbasis offline dan berdiri sendiri dan versi kedua berbasis web dengan banyak fitur di dalamnya. Silon dikembangkan untuk membantu KPU Daerah dalam melayani pendaftaran pasangan calon jalur perseorangan, meneliti dan memverifikasi syarat dukungan pasangan calon dari jalur perseorangan; 5). Sistem Informasi Logistik (Silog) adalah sebuah aplikasi berbasis website di mana setiap KPU Provinsi dan KPU Kabupaten/Kota memiliki akses untuk memberikan informasi terkait dengan proses pengadaan dan pendistribusian logistik pemilu; dan 6). Website KPU dan Jaringan Dokumentasi dan informasi hukum, merupakan sarana bagi KPU untuk berinteraksi dengan masyarakat luas, sarana untuk menyampaikan pertanggungjawaban kinerja KPU kepada publik, dan sebagai salah satu sarana sosialisasi berbagai aktivitas, produk hukum dan kegiatan terkait tahapan penyelenggaraan kepemiluan yang sedang dilaksanakan KPU.

Dalam peluncuran KPU-CSIRT, 21 Januari 2022. Kepala BSSN, Letnan Jenderal TNI (Purn). Hinsa Siburian, menjelaskan ruang siber Indonesia, bahwa ancaman pada ruang siber terdiri dari tindak kejahatan seperti hacking dan social engineering dan human error, sedangkan sifat serangan yaitu teknis dan sosial. Ancaman pada ruang siber adalah tindak kejahatan (hacking, social engineering, human error). Sifat serangan seperti Teknis (DDOS, phising, malware, dan lain-lain) 2). Sosial seperti propaganda hitam dan point and shriek Serangan siber bersifat teknis yang mengagetkan jaringan, server, aplikasi, dan database. Teknik serangan : Web defacement, phishing, sql injection, brute force attack, malware attack (ransomware), DOS dan DDOs, Man In the Middle Attack, cross site scripting dan DNS (Domain Name Server Attack).

Serangan siber bersifat sosial target: lapisan sosial berupa ide, pilihan, pendapat, emosi, tingkah laku, opini dan motivasi untuk mempengaruhi cara pikir, sistem kepercayaan dan perilaku manusia melalui visualisasi informasi sasaran dan berdampak. Dengan teknik yaitu :Propaganda hitam membuat dan menyebabkan bukti-bukti palsu melalui media sosial guna menyebabkan keresahan sosial di masyarakat; Point and shriek, mengeksploitasi isu-isu yang sangat sensitif bagi kelompok masyarakat tertentu; Pembanjiran informasi, membanjiri ruang informasi dengan informasi yang saling bertentangan sedemikian rupa sehingga publik tidak mampu menilai kredibilitas informasi suatu fenomena; *Cheerleading*, mempengaruhi kapasitas otak atau kognitif pihak sasaran agar tidak lagi mampu membedakan informasi yang kredibel dan tidak kredibel; Raiding, mengambil bentuk serangan terkoordinasi terhadap suatu arena informasi dengan tujuan untuk memadamkan pengaruh suatu opini tertentu yang sedang berkembang di masyarakat; Polarisasi mempolarisasi masyarakat ke dalam dua kategori opini yang satu sama lain bertentangan secara ekstrem.

Berdasarkan pengalaman penyelenggaraan pemilu dan pemilihan, serangan sistem informasi sering diserang disebabkan oleh faktor manusia atau pengguna. Seseorang yang memiliki keahlian akan merasa dirinya hebat apabila dapat menyerang sistem informasi. Disamping itu juga keamanan sistem informasi KPU memiliki tingkat keamanan yang kurang hal ini berdampak pada mudahnya sistem informasi diserang.

Website KPU Kabupaten Bangka Tengah pernah diretas dengan mengubah tampilan. KPU RI telah menginstruksikan terhadap migrasi website, KPU Kabupaten Bangka Tengah telah melakukan migrasi website KPU. Beberapa hari pada bulan Februari 2022,website KPU Provinsi

dan KPU Kabupaten/Kota yang telah migrasi mengalami pemeliharaan, untuk itu pihak KPU RI meminta KPU Daerah untuk melakukan backup data dan perubahan password.

Tantangan lain dari serangan siber selain fisik yaitu sosiologi seperti kekeliruan penyampaian informasi merupakan tantangan bagi KPU dalam penyampaian info kepemiluan dan pemilihan. Walaupun informasi itu berasal dari sumber terpercaya bahkan dari KPU sendiri, tidak seluruh lapisan masyarakat dapat menerima dan menyampaikan informasi itu dengan baik dan benar. Kasus yang pernah terjadi di Kabupaten Bangka Tengah sehubungan dengan informasi yang keliru yaitu penggunaan KTP-Elektronik.

Tabel 1. Negara yang mengalami serangan siber pemilu

No	Negara	Tahun	Metode yang digunakan	Target
1.	Bulgaria	2015	DDoS	Komisi Pemilihan Pusat, Kementerian
2.	Montenegro	2016	DDoS	Media, partai politik, operator jaringan seluler
3.	Filipina	2016	Perusakan dan pencurian data	Situs web komisi pemilihan, basis data pemilih
4.	Prancis	2017	*Spear phishing* 2016	Partai sosialis
5.	Ghana	2016	Defacement	Komisi Pemilihan Umum
6.	Korea Selatan	2011	DDoS	Komisi Pemilihan Umum, Kandidat, oposisi
7.	Malaysia	2013	DDoS	Kandidat, media dan oposisi
8.	Nigeria	2011	Deface	Komisi Pemilihan
9.	Rusia Federasi	2011	DDoS	Media Independen
10.	Taipei	2015	Phishing	Media dan anggota DPP
11.	Republik Ceko	2017	DDoS	Presentasi Web
12.	Slovakia	2014, 2016	DDoS	Presentasi Web
13.	Tunisa	2014	-	Sistem Pendaftaran Pemilih
14.	Ukraina	2014	DDoS	Komisi Pemilihan Ukraina
15.	Amerika Serikat	2015-2016	*Spear phishing, malware*	Pemasak, petugas, database KPU, upaya pada jaringan obama, McCain
16.	Venezuela	2017	*Insider*	Penghitungan Suara

Sumber : (European Commission, 2018)

Dampak Serangan Siber

Serangan DDOS atau *Distributed Denial of Service* pada situs jual beli tiket *online* www.tiket.com hingga PT. Global Network melaporkan adanya pembobolan situs jual beli *online* ke Badan Reserse Kriminal (Bareskrim) Polri pada 11 November 2016. Kasus ini ketika pelaku mendapatkan dana Rp. 4,1 miliar, namun pihak tiket membatalkan tiket dan membatalkan tiket dan mendapatkan *refund* sehingga kerugian sebesar Rp. 1,9 miliar (Tangkary et al., 2018:43). Modus operasi dengan melakukan penyerangan bombardir terdapat suatu *website* dengan *traffic* data yang sangat besar agar server kewalahan sehingga orang tidak bisa mengakses situs website tersebut.

Kasus kejadian di atas jika melihat pada penyelenggaraan pemilu dan pemilihan ketika situs KPU diretas. Beberapa situs KPU diretas seperti pada KPU Provinsi Jawa Timur dengan alamat https://jatim.kpu.go.id degan tampilan sebagai berikut :



Sumber : detiknews, 5 Desember 2021 https://news.detik.com/berita-jawa-timur/d-5841760/situs-kpu-jatim-diretas-minta-keadilan-kasus-novia-widyasari

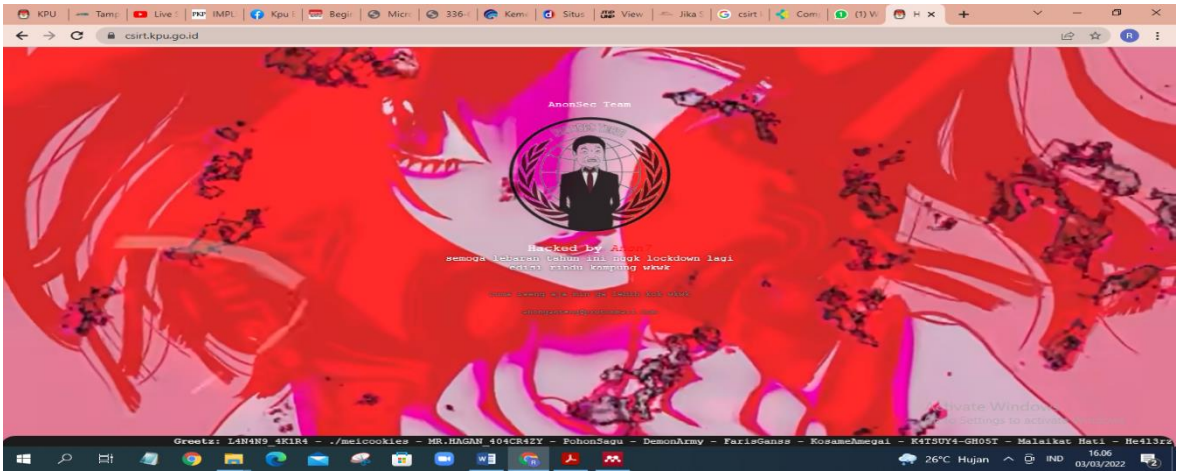
Gambar 1. Situs KPU Provinsi Jawa Timur diretas

Kasus DDOS pernah menyerang situs lindungihakpilihmu.kpu.go.id dari selasa malam 14-15 Juli 2020. Dampaknya situs yang dikembangkan oleh KPU untuk melayani pemilih yang hendak mengecek status terdaftar di dalam daftar pemilih serentak 2020. Anggota KPU RI, Viryan menyampaikan dalam diskusi "Perlindungan Data Pribadi" pada tanggal 15 Juli 2020. Mengatakan jika peretasan dan kebocoran data dapat diminimalisir karena Sidalih yang menyimpan data pemilih menggunakan sistem cermin pada situng. Server data dengan website publikasi dipisahkan sehingga ketika terjadi peretasan, peretas tidak dapat menyerang server sehingga data pemilih tetap aman.

Solusi pelaksanaan CSIRT untuk mengamankan sistem informasi pendukung pemilu dari kejahatan siber

Solusi yang dapat dilakukan yaitu pencegahan dan tanggap yang cepat. Melalui Surat Edaran KPU RI Nomor 3 tahun 2022 tentang Penerapan Kebijakan Sistem Manajemen Keamanan Informasi, melalui penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 270001:2013. Setidaknya terdapat 29 butir keamanan sistem keamanan informasi yang perlu diterapkan oleh seluruh Satuan Kerja KPU Provinsi/KIP Aceh dan KPU/KIP Kabupaten/Kota. Secara garis besar terdapat upaya untuk mengamankan sistem manajemen informasi yaitu :1). Menginstal dan *update* anti virus; 2). Pastikan USB aman; 3). Gunakan aplikasi resmi dan berlisensi; 4). Gunakan Enkripsi; 5). *Back Up* data secara teratur; dan 6). Inventarisasi perangkat, pengguna dan peruntukannya.

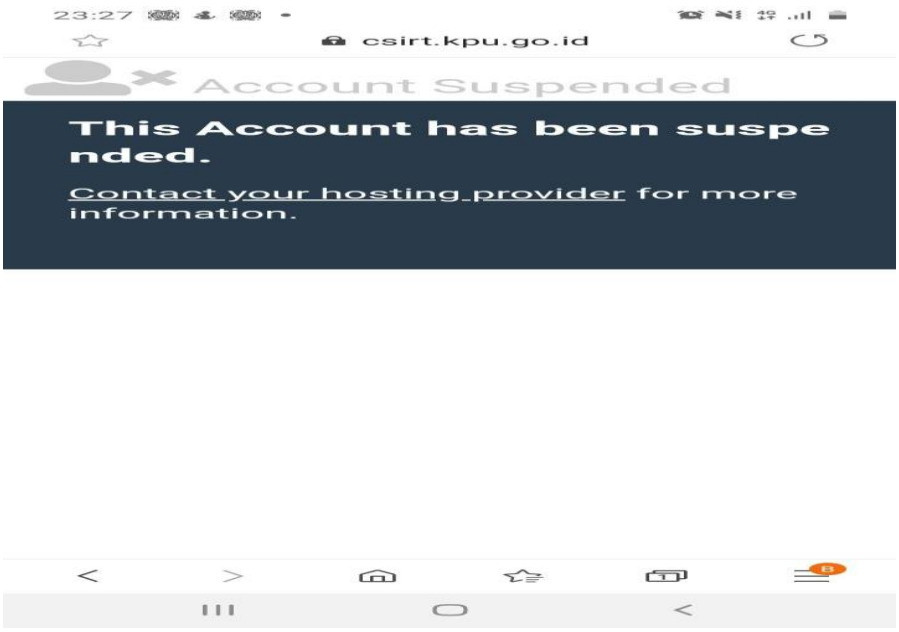
Upaya pengamanan sistem informasi dapat dilakukan dengan komunikasi antar satuan kerja KPU di daerah. Seperti pada kasusHingga dalam pencarian informasi KPU-CSIRT, ternyata laman KPU-CSIRT diretas yaitu sebagai berikut:



Sumber : Layar Tangkap www.KPU-CSIRT.go.id , 03 Maret 2022

Gambar 2. Halaman CSIRT KPU diretas

Selanjutnya, saya pun menghubungi teman KPU RI yang berada di Biro Pusat Data dan Informasi (pusdatin), dan langsung ditanggapi dengan melakukan tampilan seperti di bawah ini :



Sumber: layar tangkap KPU-CSIRT yang sedang ditutup

Gambar 3. KPU-CSIRT sedang ditutup

Sehingga keberadaan KPU-CSIRT dengan melibatkan keberadaan KPU Daerah sangat diperlukan dalam mendeteksi beberapa ancaman dan keamanan siber. Selain itu juga laman BSSN juga pernah diretas seperti pada tampilan di bawah ini



Sumber : layar tangkap www.pusmana,bssn.go.id

Gambar 4. Laman BSSN diretas

Situs BSSN beralamat www.pusmana.bssn.go.id yang merupakan website untuk pusat Malware Nasional, peretasan telah ditangani oleh tim terkait. Sub Domain situs resmi BSSN tersebut langsung ditangani tim *Computer Security Incident Response Team* (CSIRT) dari BSSN.

Serangan pada website dengan mengubah tampilan seperti font *website* diganti, muncul iklan mengganggu hingga perubahan konten jalanan seluruh

> "Kalau dicek attack-nya,mungkin bisa dicari tahu kenapa bisa firewall-nya mem-bypass serangan ke cela vulnerable-nye. Attack yang simple pun kalau lolos dari firewall bisa mengakibatkan kerusakan yang besar. Jangan dianggap semua serangan deface itu serangan ringan, bisa jadi hacker sudah masuk sampai ke dalam" kata Chairman (BSSN)

Kejahatan siber secara klarifikasi terdiri dari 2 jenis yaitu *insider attack* dan *eksternal attack* (Darmayani, 2021:14). Serangan *insider* yaitu didalangi oleh orang dalam harus menjadi perhatian karena secara kelembagaan KPU terdiri dari para pegawai yang tetap dan kontrak, potensi terjadi jika penguatan SDM dengan melakukan audit SDM seperti ketika seorang pegawai bukan menjadi pegawai KPU maka kewajiban dan wewenangnya juga harus dihilangkan karena akan ada kekhawatiran akan adanya serangan dari dalam.

Kasus yang paling dikhawatirkan adalah serangan secara sosiologis melalui media sosial dan kesalahan penerapan (Ulzikri, 2022). Beberapa contoh pada pemilu 2019 kemarin telah terjadi kesalahpahaman terhadap sesuai seperti pada kasus salah satu penyebab terjadinya Pemungutan Suara Ulang di Kabupaten Bangka Tengah kesalahan pemahaman informasi penggunaan KTP-Elektronik untuk pemungutan suara, sehingga pemilih luar bersitegang dengan pengawas TPS dan KPPS dalam penggunaan suara.yaitu

pada TPS 10 Desa Beluluk dan TPS 4 Desa Air Mesu Kecamatan Pangkalan Baru, dampak pelanggaran administrasi penyebab PSU (Febriansyah, dkk, 2021:74)

Tentu ancaman keamanan siber terdiri dari 2 jenis yaitu secara fisik dan sosial. Ketika terjadi ancaman maka dapat dilakukan dengan respon yang cepat, hal ini bertujuan untuk memberikan kepercayaan publik akan proses pemilu dan pemilihan yang transparan, akuntabel dan dipercaya publik. Kedua ancaman tersebut masing-masing memiliki dampak yang sangat signifikan terhadap penyelenggaraan pemilu dan pemilihan. Terutama bagi penyelenggara pemilu khususnya KPU. Sebagai penyelenggara pemilu KPU dituntut untuk menyelenggarakan pemilu dan pemilihan yang mana pada tahun 2024 akan diselenggarakan di tahun yang sama.

Potensi masalah yang bakal di hadapi dalam pelaksanaan CSIRT

Terdapat potensi masalah dalam pelaksanaan KPU-CSIRT seperti anggaran, Sumber Daya Manusia (SDM) dan Infrastruktur.

a. Anggaran

Anggaran yang fantastis diusulkan oleh KPU menuai pro dan kontra publik, terlebih pemerintah masih fokus dalam penanggulangan pandemi covid-19. KPU telah mengusulkan anggaran sebesar Rp. 86 Triliun, apabila melihat perbandingan pemilu 2019 sebesar Rp. 25,29 Triliun dan anggaran pemilu 2014 hanya Rp. 15,62 triliun. Dalam 2 (dua) kali penyelenggaraan pemilu, anggaran mengalami peningkatan yang sangat signifikan, anggaran pemilu serentak 2024 mengalami kenaikan 3 (tiga) kali lipat pada pemilu sebelumnya. KPU RI menanggapi jika usulan anggaran mengalami kenaikan 3 (tiga) kali lipat karena digunakan untuk pembangunan infrastruktur, sarana dan prasarana agar pada pemilu 2024 berjalan dengan baik. Ketua KPU RI, Ilham Saputra menyampaikan jika anggaran ini masih kami bicarakan dan rasionalisasikan, tapi KPU berkomitmen mengembangkan sarana dan prasarana KPU di Kabupaten/kota dan Provinsi. Beberapa prioritas penggunaan anggaran untuk pemilu 2024 diantaranya pembangunan kantor KPU di daerah; mengembangkan perhitungan rekapitulasi suara; dan mengajukan kenaikan honor untuk para petugas pemilu 2024. Sementara Menteri Dalam Negeri, Tito Karnavian, mengungkapkan perlu adanya *exercise* dan betul-betul melihat detail satu per satu anggaran pemilu 2024 tersebut, karena ini merupakan lompatannya terlalu tinggi.

b. Sumber Daya Manusia (SDM)

Penguatan SDM dapat meliputi peningkatan keahlian seperti mengikuti *workshop, cyber security drill* dan pelatihan sejenisnya. Tujuannya untuk meningkatkan kualitas SDM dalam menangani insiden keamanan Siber. KPU RI telah melakukan berbagai rangkaian kegiatan pelatihan CSIRT bekerja sama dengan BSSN. Tentu KPU perlu memberikan pemahaman kepada SDM yang berada di daerah karena jika terjadi insiden keamanan siber, KPU Daerah yang akan membuat laporan dan mendeteksi keamanan siber tersebut.

Menjadi permasalah bagaimana struktur CSIRT KPU bekerja dari semua ancaman yang akan menyerang tentu diperlukan respon yang cepat dalam mengatasi keamanan siber. Selain untuk membentuk CSIRT, para pegawai merupakan operator berbagai macam sistem informasi, karena sifatnya tanggap maka perlu adanya respon 24/jam. KPU-CSIRT

harus melayani 34 KIP Provinsi/KPU Provinsi dan 514 KIP/KPU Kabupaten/kota. Dengan total satuan kerja sebanyak 548, tentu tim KPU-CSIRT akan kewalahan dalam menghadapi dan merespon insiden yang terjadi di KPU Daerah.

SDM perlu mendapatkan bimbingan teknis dan pelatihan. Selama pandemi biasa dilakukan secara daring tentu tidak berjalan efektif karena memerpulan praktek langsung ke lapangan. Jika pelatihan dilakukan secara daring tentu tidak berjalan efektif. Kedepannya bimbingan teknis dan berbagai pelatihan dapat dilaksanakan dengan tatap muka dengan tetap menerapkan protokol kesehatan yang ketat.

KPU Kabupaten Bangka Tengah terdiri dari unsur komisioner dan sekretariat yang memiliki kompetensi keilmuan dan pengalaman dalam bidang pemilu dan teknologi informasi, sekretariat tersebar dalam beberapa operator seperti sipol, sidalih dan lain-lain. Selain pendidikan berlatar belakang teknologi Informasi, para pegawai KPU juga pengalaman berbagai operator sistem informasi KPU.Dengan menerapkan KPU-CSIRT jika terjadi insiden dapat melakukan laporan dan perlu tanggapan dari tim KPU-CSIRT pusat.

KPU Kabupaten Bangka Tengah sudah mengikuti pemahaman Peraturan Komisi Pemilihan Umum Nomor 5 tahun 2021 yang diselenggarakan oleh KPU Provinsi Kepulauan Bangka Belitung. Pencegahan, KPU telah mengeluarkan SE Nomor 3 tahun 2022 tentang Penerapan Kebijakan Sistem Manajemen Informasi dengan memuat 29 poin yang wajib dilakukan oleh KPU Provinsi dan KPU Kabupaten/Kota dalam penerapan kebijakan SMKI berdasarkan Standar ISO/IEC 27001:2013. Dengan telah dibentuknya CSIRT KPU maka penerapan SMKI dapat dilakukan sebagai tim gerak cepat yang dibentuk untuk menangani kejadian-kejadian yang terkait dengan keamanan informasi dan insiden siber.

c. Infrastruktur

Melalui Surat Edaran KPU RI Nomor 3 tahun 2022 tentang Penerapan Kebijakan Sistem Manajemen Keamanan Informasi, melalui penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 270001:2013. Setidaknya terdapat 29 butir keamanan sistem keamanan informasi yang perlu diterapkan oleh seluruh Satuan Kerja KPU Provinsi/KIP Aceh dan KPU/KIP Kabupaten/Kota. Secara garis besar terdapat upaya untuk mengamankan sistem manajemen informasi yaitu :1). Menginstal dan *update* anti virus; 2). Pastikan USB aman; 3). Gunakan aplikasi resmi dan berlisensi; 4). Gunakan Enkripsi; 5). *Back Up* data secara teratur; dan 6). Inventarisasi perangkat, pengguna dan peruntukannya.

Infrastruktur KPU dalam mendukung KPU-CSIRT sebagai wujud penerapan SPBE. KPU memiliki server fisik sebanyak 44 unit dan s*erver virtual machine* sebanyak 177 unit, perangkat jaringan sebanyak 63 unit dengan rincian *router* berjumlah 3 unit berfungsi untuk penghubung jaringan internet kepada 1 atau lebih perangkat, *switch* berjumlah 27 unit berfungsi sebagai penghubung sejumlah perangkat komputer untuk melakukan pertukaran paket serta meneruskan data ke berbagai perangkat tujuan, *access point* berjumlah 33 unit berfungsi sebagai penyebar sinyal internet kepada perangkat melalui gelombang radio. KPU juga memiliki data center sebanyak 1330. Dengan infrastruktur ini, KPU menerapkan SPBE melalui berbagai informasi yang telah

dikembangkan. Tetapi infrastruktur yang berada di KPU RI perlu ditopang dengan ketersediaan infrastruktur di KPU Daerah. Dalam penerapan SPBE di KPU Kabupaten Bangka Tengah, memiliki berbagai perangkat keras *(hardware)* seperti Komputer, Laptop dan sarana internet. KPU Kabupaten Bangka Tengah belum memiliki jaringan intranet dan server. Sehingga untuk melakukan *backup* data penyimpanan melalui *harddisk* eksternal dan melakukan "burning" DVD untuk arsip digital. Kedepannya diperlukan server untuk mendukung penerapan SPBE yang efektif, efisien dan kondusif. Selama pengalaman penggunaan sistem informasi, terlebih pada *bandwidth* yang sedang padat sering lambat dan kurang berjalan efektif. Melalui *backup* data merupakan suatu bentuk sistem keamanan sistem manajemen informasi ketika terjadi serangan siber dan data KPU Kabupaten Bangka Tengah diserang, KPU Kabupaten Bangka Tengah memiliki *"backip"* data.

Strategi pelaksanaan CSIRT

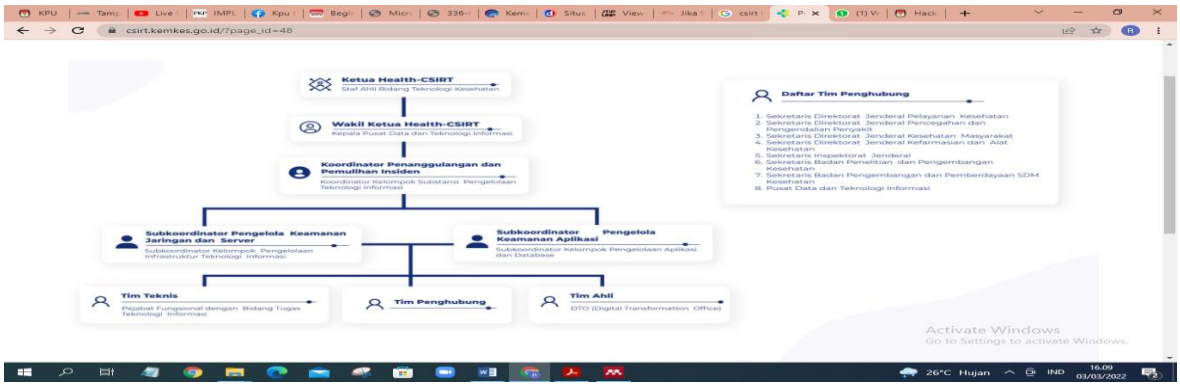
KPU harus bergerak cepat dalam penerapan CSIRT demi melakukan pengamanan sistem informasi terutama dalam persiapan pemilu dan pemilihan serentak 2024 nanti. Terdapat beberapa strategi yang dapat dilakukan untuk pelaksanaan CSIRT yaitu mendesain CSIRT, menerapkan SPBE yang optimal dan melakukan kolaborasi dengan Kementerian/Lembaga dan Pemerintah Daerah yang berhubungan dengan keamanan siber.

a. Desain CSIRT

Dalam pembentukan CSIRT dasar hukum pembentukannya tertuang dalam Pembukaan Undang‑Undang Dasar Negara Republik Indonesia Tahun 1945 pada alenia ke-4 yaitu "melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia". Dimasa kemajuan teknologi informasi, data menjadi penting dalam perlindungannya sehingga tugas negara yaitu melindungi segenap bangsa Indonesia. Pada Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Undang-Undang Nomor 11 tahun 2008. Selanjutnya Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik. Peraturan Presiden Republik Indonesia Nomor 28 tahun tentang Badan Siber dan Sandi Negara.

Data BSSN Menunjukan hingga bulan Desember 2021, terdapat lebih dari 1 minimalis serangan siber di Indonesia hal ini dipicu salah satunya peningkatan implementasi layanan berbasis elektronik sebagai pemicu kejahatan siber (Sudarmadi & Runturambi, 2019:171) memberikan rekomendasi strategi BSSN dalam menghadapi ancaman siber yaitu salah satunya meningkatkan kerjasama keamanan siber. Dalam hal ini keamanan siber pemilu milik KPU dapat direalisasikan dengan KPU-CSIRT. Program BSSN pada CSIRT melalui sektor pemerintah yaitu : 1). Asistensi pembentukan CSIRT; 2). Pembentukan CSIRT; 3). Peningkatan kapasitas CSIRT; dan 4). Peningkatan Kematangan CSIRT.

Kementerian Kesehatan (Kemenkes) merupakan salah satu Kementerian yang telah terbentuk CSIRT termasuk 15 kementerian/lembaga dan pemerintah pada tahun 2020. Berikut ini struktur organisasi CSIRT yang telah terbentuk :



Sumber : Layar Tangkp www.csirt-kemekes.go.id

Gambar. 5 Struktur organisasi CSIRT- Kemenkes

b. Penerapan SPBE

Pembentukan CSIRT sejalan dengan penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Bagian unsur keamanan SPBE meliputi penjaminan kerahasiaan, keutuhan, dan ketersediaan data dan informasi sehingga pesan CSIRT sebagai monitor dan penyedian pemulihan dari insiden keamanan siber. SPBE merupakan penyelenggaraan pemerintah yang memanfaatkan teknologi dan komunikasi untuk memberikan layanan kepada pengguna SPBE. Sesuai dengan Peraturan Presiden Nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. SPBE bertujuan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, dan transparan, dan akurat serta pelayanan publik yang berkualitas dan terpercaya. KPU sendiri telah membentuk Peraturan Komisi Pemilihan Umum Nomor 5 tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum. Secara nasional SPBE terdiri dari tim koordinasi yaitu Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (Menpan-RB) sebagai ketua tim Koordinasi, anggota tim koordinasi terdiri dari Menteri Dalam Negeri, Menteri Keuangan,Menteri Komunikasi dan Informatika, Menteri PPN atau Bappenas, Kepala Badan Siber dan Sandi Negara dan Kepala Badan Pengkajian dan Penerapan Teknologi. Dengan adanya SPBE ini, kepala BSSN bertanggung jawab dalam penyusunan standar keamanan nasional, menetapkan manajemen keamanan dan melaksanakan audit keamanan SPBE Nasional. BSSN merupakan wujud dalam memfasilitasi kinerja dan memfasilitasi CSIRT bagi Kementerian, Lembaga dan Pemerintah Provinsi.

SPBE memiliki visi terwujudnya sistem pemerintahan berbasis elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan publik yang berkinerja tinggi sesuai dengan Peraturan Presiden Nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Dalam penyelenggaraan pemilu dan pemilihan, KPU memanfaatkan teknologi informasi dalam penyelenggaraan tahapan pemilu dan pemilihan. Berbagai macam sistem informasi yang diterapkan oleh KPU (Rizkyansyah, 2019:282-284).

1. Sistem kepemiluan (Election System); portal seperti SIDAPIL, SIDALIH, SIPOL, SILOG, SITAP, SI Wilayah, SITUNG, SIANG, SIGAS, SIGEOM SIAKUR dan SIPAW.

2. Sistem Administrasi (*Administration System)* merupakan kumpulan aplikasi yang berfungsi untuk mendukung aktivitas-aktivitas internal yang mana tidak berhubungan dengan aktivitas kepemiluan, seperti SIADKA, SIM2P, dan E-Kolaborasi, E-Money, SIADKA, SIM2P, SIPRENJA, SIMONIKA/Keuangan, SIASET, Helpdesk, SIJADWAL dan SI audit.
3. Sistem Manajemen Pengetahuan (*Knowledge Management System*) merupakan kumpulan sistem informasi yang berfungsi untuk mengelola aset informasi dan pengetahuan yang dimiliki oleh KPU. Beberapa aplikasi seperti JDIH, e-collaboration, e-documents dan tacit knowledge.
4. Pengelolaan Data (*Data Governance*) merupakan konsep atau kerangka kerja yang diimplementasikan KPU untuk menjaga kualitas data.
5. Sistem Informasi Eksekutif (*Executive Information System)* merupakan kumpulan aplikasi yang digunakan sebagai pendukung keputusan yang dibutuhkan oleh para eksekutif dari pimpinan KPU. Inisiatif yang tergolong dalam domain ini adalah master data, data warehouse, dan dashboard.
6. Kanal Akses (*Acces Channel*) merupakan kumpulan teknologi kanal atau *channel* yang berfungsi untuk mendukung pertukaran data dan informasi yang dimiliki oleh KPU dengan para pemangku kepentingan lainnya. Beberapa teknologi yang dikategorikan ke dalam *acces* channel yaitu *portal/website, open data, helpdesk* dan *call center.*

Dengan menggunakan berbagai sistem informasi tersebut KPU telah menerapkan SPBE. Sebagai lembaga penyelenggara pemilu yang menyelenggarakan pemilu dan pemilihan di tingkat pusat dan daerah. KPU menerapkan SPBE melalui berbagai macam sistem informasi untuk memberikan pelayanan kepada pemilih, peserta berupa partai politik dan pasangan calon dan juga masyarakat umum. Tentunya sistem yang dikembangkan memerlukan koordinasi yang baik tingkat KPU RI, KPU Provinsi dan KPU Kabupaten/Kota melalui divisi dan sub koordinator.

CSIRT sangat perlu diterapkan di kementerian/lembaga dan pemerintah daerah. Seperti kasus kebocoran data e-HAC (*electronik- Health Alert Card*), ketika pelapor kebocoran data melaporkan ke Kementerian Kesehatan (Kemenkes) tetapi tidak ditindaklanjuti dan baru ketika melaporkan ke BSSN, laporannya ditindaklanjuti (Jurnal Security, 2021). Dengan demikian keberadaan CSIRT sangat diperlukan di tengah meningkatnya penggunaan internet sekarang ini.

Peluncuran CSIRT merupakan kerjasama antara KPU dan BSSN sebagai persiapan pemilu dan pemilihan 2024 serta pengalaman pemilu 2019 adanya kebocoran data dan insiden pemilu.

> "Saya kira gerak cepat KPU bersama BSSN untuk mengembangkan CSIRT dari BSSN bekerja sama dengan KPU berfungsi untuk merespon dan mitigasi ketika terjadi insiden siber yang pengalamn tadi sehingga diharapkan penerapan SPBE pada KPU RI menjadi semakin efektif ". (Tanggapan dari Ketua KPU RI tentang CSIRT, 21 Januari 2022".

Melalui BSSN sebagai organisasi yang bertanggung jawab dalam bidang keamanan siber di Indonesia dan bertindak sebagai CERT Nasional, selalu melaksanakan integrasi, koordinasi, harmonisasi instansi pemerintah, infrastruktur informasi kritis nasional, sektor swasta dan masyarakat sipil dalam penyelenggaraan keamanan siber di Indonesia.(Sudarmadi dan Runturambi, 2019:168). Melalui struktur organisasi dan tim yang bertugas maka ketika terjadi insiden keamanan siber, tim dapat bekerja untuk menanggulanginya. Sekarang ini KPU-CSIRT masih berada ditingkat pusat dan masih melakukan kerjasama dengan BSSN.

c. Bekerjasama dengan CSIRT Kementerian/Lembaga dan Pemerintah Daerah

KPU-CSIRT telah terdaftar melalui surat tanda registrasi Nomor :054/CSIRT.01.01/BSSN/01/2022, tanggal 21 Januari 2022. KPU telah terdaftar pada CSIRT-BSSN pada tahun 2022. Pembentukan 131 CSIRT pada tahun 2020-2024, di tahun 2020 telah terbentuk CSIRT di 15 Kementerian/Lembaga dan Daerah, di tahun 2021 telah terbentuk sebanyak 39 Kementerian/Lembaga dan Daerah. Pada tahun 2022 ini, KPU-CSIRT bersama 32 Kementerian/Lembaga Daerah dibentuk. Dengan demikian, KPU dapat bekerjasama dengan Kementerian/Lembaga dan Daerah yang telah dulu terbentuk CSIRT.

Layanan tambahan pembangunan kesadaran dan kepedulian terhadap keamanan siber. Ancaman pada ruang siber meliputi tindak kejahatan (*hacking* dan *social engineering*), *Human Error*. Sifat serangan meliputi teknis seperti DDoS, *Phishing*, *Malware*). Sosial seperti Propaganda hitam, point and shriek. Ancaman berita hoax dan serangan siber masih menjadi tantangan dalam penerapan CSIRT. Beberapa kali keamanan sistem pemilu KPU diserang oleh *hacker*. Pada kasus *website* csirt.kpu yang diserang maka tim CSIRT dapat merespon, mendeteksi dan mitigasi serangan *website* tersebut. Tentu peran KPU Daerah perlu jika terjadi ancaman dan serangan siber yang tiba-tiba menyerang. Selain itu KPU dapat berkomunikasi dengan BSSN, Polisi Republik Indonesia (Polri) dan Kementerian Komunikasi dan Informatika (Kominfo) yang memiliki otoritas. Belajar dari pengalaman CSIRT-BSSN yang pernah menanggapi respon ketika *website* diretas.

KPU-CSIRT melalui tugas pokok dan fungsinya dapat merespon ketika terjadi insiden keamanan siber. KPU-CSIRT bertujuan melindungi data, identitas dan administrasi sistem kepemiluan dari ancaman kebocoran data, maka implementasi KPU-CSIRT yaitu :1). Melakukan koordinasi dengan Gov-CSIRT (BSSN) dalam merespon insiden yang terjadi; 2). Monitoring perangkat keamanan dalam upaya mendeteksi anomali yang terjadi; dan 3) melakukan mitigasi terhadap insiden serangan siber yang terjadi. CSIRT- KPU berada di tingkat KPU RI dan berkoordinasi BSSN tentu kedepannya KPU dapat melakukan pembentukan CSIRT dengan melibatkan KPU Provinsi dan KPU Kabupaten/Kota

Keberadaan badan *ad hoc* meliputi PPK, PPS dan KPPS. Tentu jika terjadi insiden di tingka badan *adhoc* , CSIRT KPU belum mampu untuk melayaninya, sehingga keberadaan KPU Kabupaten/kota dapat menanggapi jika terjadi insiden. Tentu KPU Kabupaten/kota diberikan hak dan kewenangan dalam membuat kebijakan penanggulangan insiden keamanan pemilu.

KESIMPULAN

KPU-CSIRT merupakan upaya KPU dalam mengamankan sistem informasi yang dikembangkan oleh KPU. Dengan KPU-CSIRT, ketika terjadi insiden keamanan pemilu maka tim dapat merespon dengan cepat, tepat dan aman sehingga berjalan kondusif. Meningkatnya penggunaan teknologi tentu menjadi tantangan KPU dalam pengamanan siber, tantangan seperti anggaran, desain CSIRT dan pengembangan SDM serta masih adanya ancaman keamanan siber KPU. Pemilu 2024 nanti, terutama di Kabupaten Bangka Tengah yang telah menyelenggarakan pemilu 2019 dan pemilihan 2020 tentu masih akan ada ancaman keamanan siber secara nasional tentu akan berdampak juga di Kabupaten Bangka Tengah. Pengembangan CSIRT dari KPU, KPU Provinsi dan KPU Kabupaten/Kota terlebih KPU telah menetapkan PKPU tentang Penerapan Sistem Informasi Berbasis Elektronik. Dengan penerapan tanggap dan respon ketika terjadinya insiden tentu kepercayaan publik akan proses dan hasil pemilu dapat dipertanggungjawabkan untuk legitimasi hasil pemilu tersebut.

Pembentukan struktur organisasi KPU-CSIRT yang cepat dan tanggap dari KPU, KPU Provinsi dan KPU Kabupaten/Kota hingga badan adhoc PPK, PPS dan KPPS. Pada penyelenggaraan hari pemungutan suara, penghitungan dan rekapitulasi suara ketika terjadi insiden harus cepat merespon karena jika tidak akan terjadi kesalah Infrasturkutpahaman dan ketidak percayaan publik dari hasil pemilu apalagi anggaran besar yang diajukan oleh KPU salah satunya pengembangan sistem informasi penghitungan suara. CSIRT ada juga di kementerian/lembaga dan pemerintah daerah, bagi yang sudah teregistrasi, KPU dapat berkolaborasi bersama untuk pengamanan siber pemilu Seperti Kominfo, Polri, TNI dan Pemerintah Daerah. Meminimalisasi serangan siber dengan penerapan keamanan siber melalui kebijakan Sistem Manajemen Informasi sesuai SE nomor 3 tahun 2022, dimana terdapat poin penting untuk seluruh KPU Provinsi/KIP Aceh dan KPU/KIP Kabupaten/Kota dalam hal sistem keamanan informasi dan kebersihan siber secara efektif, efisien, dan konsisten..

REFERENSI

Agustini, P. (2021). Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya di Internet. Kementerian Komunikasi Dan Informatika.

Anjani, N. H. (2021). Perlindungan Keamanan Siber di Indonesia. Ringkasan Kebijakan, 9, 1–12.

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. Politica, 5(1), 95–110.

Astuti, A. M. I., & Ratnawati, S. (2020). Analisis SWOT Dalam Menentukan Strategi Pemasaran (Studi Kasus di Kantor Pos Kota Magelang 56100). Jurnal Ilmu Manajemen, 17(2), 58–70.

Bada, Maria, etc. (2014). Computer Security Incident Response Teams (CSIRTs) An Overview. In Global Cyber Security Capacity Centre (Vol. 3, Issue May). University of Oxford. https://doi.org/10.1002/9781118256107.ch39

Bouty, A. A., Koniyo, M. H., & Novian, D. (2019). Evaluasi Sistem Pemerintahan Berbasis Elektronik Menggunakan E-Government Maturity Model (Kasus di Pemerintah Kota Gorontalo). Jurnal Penelitian Komunikasi Dan Opini Publik, 23(1). https://doi.org/10.33299/jpkop.23.1.1758

BSSN. (2022). BSSN dan KPU Berkolaborasi Membentuk KPU-CSIRT untuk Mengamankan Sistem Pemilihan Umum dari Kejahatan Siber.

Ellena, K., Petrov, G., & Bloom, R. (2018). Cybersecurity in Elections Cybersecurity in Elections (Issue October).

European Commission. (2018). Compendium on Cyber Security of Elections Technology. July, 51. https://www.ria.ee/public/Cyber_security_of_Election_Technology.pdf

Goeritno, A., & Hendrawan, A. H. (2016). Implementasi Iso / Iec 27001 : 2013 Untuk Sistem Manajemen Keamanan Informasi (Smki) Pada Fakultas Teknik Uika-Bogor. Seminar Nasional Sains Dan Teknologi Fakultas Teknik Universitas Muhammadiyah Jakarta, 8(November), 1–5. https://media.neliti.com/media/publications/174077-ID-none.pdf

Hayaty, N. (2020). Buku Ajar: Sistem Keamanan.

Hendra, R., & Hanita, M. (2020). The Implementation of Cyber Incident Management Frameworks in Indonesia. Jurnal Teknologi Informasi Dan Pendidikan, 13(2), 9–16. https://doi.org/10.24036/tip.v13i2.326

Kurnia, F. R. M. B. (2019). Tata Kelola Pemilu di Indonesia. KPU RI.

Nist. (2018). Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Penting. www.onlinedoctranslator.com

Nugroho, K., & Liando, F. D. M. (2019). Tata Kelola Pemilu di Indonesia. In Tata Kelola Pemilu di Indonesia.

Pratama, Heroik, Amalia Salabi, N. (2019). Panduan Penerapan Teknologi Pungut-Hitung di Pemilu (Buku Panduan untuk Indonesia). Perludem.

Pratiwi, H. D., Hayuhardhika, W., Putra, N., & Herlambang, A. D. (2020). Evaluasi Penerapan E-Government Di Pemerintah Kabupaten Sumbawa Besar Menggunakan Kerangka Kerja Sistem Pemerintahan Berbasis Elektronik (SPBE). Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 4(11), 4116–4124.

Setiawan, A. B. (2013). Perencanaan Strategis Pembentukan Pusat Respon Insiden Keamanan Informasi Pemerintah. JURNAL IPTEKKOM : Jurnal Ilmu Pengetahuan & Teknologi Informasi, 16(1), 27. https://doi.org/10.33164/iptekkom.15.1.2013.27-46

Setiawan, A. B. (2015). Kajian Strategi Pengamanan Infrastruktur Sumber Daya Informasi Kritis. Buletin Pos Dan Telekomunikasi, 1(1), 45. https://doi.org/10.17933/bpostel.2015.130104

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 2(2), 157–178. http://jurnalpkn.ui.ac.id/index.php/jkskn/article/view/28

Nugroho, K., & Liando, F. D. M. (2019). Tata Kelola Pemillu di Indonesia. In *Tata Kelola Pemilu di Indonesia*.

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157–178.

Ulzikri, A. R. (2022). Efektifitas Strategi Kampanye Politik Melalui Media Sosial : Belajar Pada Pilkada Bandar Lampung Tahun 2020. *Jurnal Ilmu Politik Dan Studi Sosial Terapan (JIPOSSTER)*, *1*(1), 1–13.

Zed, M. (2014). Metode Penelitian Kepustakaan (ke-3). Yayasan Obor Indonesia.