KONFERENSI NASIONAL
ILMU ADMINISTRASI 8.0
"Penguatan Kebijakan dan Kelembagaan Untuk Mendukung Pembangunan Berkelanjutan di Era Transformasi Nasional"
29 AGUSTUS 2024 POLITEKNIK STIA LAN BANDUNG
E-ISSN : 2988-5485 (online)

Tata Kelola Keamanan Siber Untuk Mencegah dan Mengatasi Ancaman Kejahatan Siber Pemilu

Ricky Febriansyah[a] , Ana Husnayanti [b]

[a] Sekretariat KPU Kabupaten Bangka Tengah -Koba
[b] Poltekkes Kemenkes Pangkapinang - Pangkalpinang
e-mail : [a] ricky.febriansyah290284@gmail.com , [b] mahardhera@gmail.com

Abstrak

Kasus kejahatan siber pada pemilu serentak 2019 dan 2024 dapat menjadikan tolak ukur bahayanya kejahatan siber. Tujuan penelitian ini adalah bagaimana tata kelola keamanan siber upaya pencegahan dan mengatasi ancaman kejahatan siber pemilu. Dengan menggunakan metode penelitian kualitatif deskriptif melalui kajian pustaka dari regulasi, jurnal dan buku serta materi narasumber *webinar* forum koordinasi, dan sinkronisasi dari Badan Siber dan Sandi Negara (BSSN), Badan Intelijen Negara (BIN), Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dan KPU. Penelitian ini menghasilkan 2 (dua) pembahasan yaitu 1). Ancaman Serangan Siber Pemilu terdiri dari 3 (tiga) meliputi infrastruktur, situs KPU, dan Konten Negatif; 2). Pencegahan dan Mengatasi ancaman kejahatan siber pemilu melalui tata kelola keamanan siber melalui kebijakan pembuatan regulasi. BSSN, BIN, KPU, TNI, Polri dan Kominfo. Peraturan KPU Nomor 5 Tahun 2021 tentang Sistem Pemerintah Berbasis Elektronik (SPBE). Peran BSSN sangat penting melalui tim operasi pengamanan pemilu. Desk Koordinasi pemilu bidang Politik Hukum dan Keamanan dalam menghadapi serangan siber yang bersifat sosial, teknik dan saluran transmisi serta ancaman serangan pemilu melalui infrastruktur jaringan, situs website KPU, dan Penyebaran konten negatif.

Kata Kunci: Badan Siber Sandi Negara (BSSN), Keamanan Siber, Kejahatan Siber Pemilu, Komisi Pemilihan Umum (KPU)

Cyber Security Governance to Prevent and Overcome the Threat of Election Cyber Crime

Abstract

Cybercrime cases in the 2019 and 2024 simultaneous elections can be used as a benchmark for the dangers of cybercrime. The aim of this research is how cyber security governance can prevent and overcome the threat of election cyber crime. By using descriptive qualitative research methods through literature reviews from regulations, journals and books as well as resource material for webinars, coordination forums, and synchronization from the National Cyber and Crypto Agency (BSSN), the State Intelligence Agency (BIN), the Association of Indonesian Internet Service Providers (APJII) and KPU. This research resulted in 2 (two) discussions, namely 1). Election Cyber Attack Threats consist of 3 (three) including infrastructure, KPU sites, and Negative Content; 2). Preventing and overcoming the threat of election cyber crime through cyber security governance through policy making regulations. BSSN, BIN, KPU, TNI, Polri and Kominfo. KPU Regulation Number 5 of 2021 concerning Electronic-Based Government Systems (SPBE). The role of BSSN is very important through the election security operations team. Election Coordination Desk in the field of Political, Legal and Security in dealing with social, technical and transmission channel cyber attacks as well as the threat of election attacks through network infrastructure, KPU websites, and the negative content.

Keywords: *National Cyber and Crypto Agency BSSN, Cyber Security, Election Cyber Crime, General Election Commission (KPU).*

E-ISSN : 2988-5485 (online)

A. PENDAHULUAN

Ancaman kejahatan tidak saja berada di dunia nyata akan tetapi di dunia maya atau di dunia digital. Istilah kejahatan ini disebut kejahatan siber atau *cyber crime.* Menurut Aldo (2020) kejahatan siber adalah kejahatan yang ditimbulkan karena pemanfaatan teknologi internet. Kejahatan ini pun akan meningkat dengan banyaknya pengguna internet dalam setiap sisi kehidupan masyarakat. Ancaman tersebut menjadi salah satu risiko dalam sebuah organisasi tidak terkecuali organisasi publik (Pradesa et al., 2023; 2021). Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) secara resmi merilis hasil survei Penetrasi Internet Indonesia mencapai 215,63 juta orang pada periode 2022-2023. Dampak dari tingginya pengguna internet terjadinya peningkatan tindak pidana kejahatan siber yang hingga 14 kali. Data dari e-MP Robinopsnal Bareskrim Polri, Kepolisian telah menindak sebanyak 8.831 kasus kejahatan siber sejak tanggal 1 Januari hingga 22 Desember 2022.

Dampak dari kejahatan siber yang pasti adalah kerugian finansial seperti penipuan *online,* peretasan dan *skimming* kerugian bagi korban atas kehilangan uang atau aset lainnya. Seperti contoh dalam kasus kebocoran data informasi pribadi bagi para konsumen pada *e-commerce* Tokopedia yang mengalami kebocoran 91 (sembilan puluh satu) juta akun data pribadi dan 7 (tujuh) akun penjual atau *merchant* (Dal, 2020). Kasus lain yang tidak kalah menghebohkan kejahatan siber dari Grab Toko yang melakukan penipuan kepada konsumen sebanyak 980 orang dengan total kerugian mencapai Rp. 17.000.000.000,- (tujuh belas miliar rupiah) (Uli, 2021). Baru-baru ini di tahun 2023 kasus kejahatan siber di Indonesia sangat menggemparkan publik seperti hacker Bjorka, kebocoran data BPJS Ketenagakerjaan mencapai 18,5 juta data pengguna yang dijual ke forum gelam seharga Rp.153 juta. Kasus yang tidak dapat dilupakan oleh nasabah Bank Syariah Indonesia (BSI). Total data yang dicuri mencapai 1,5 TB termasuk juga 15 juta data pengguna dan password untuk akses internal dan layanan serta data pribadi nasabah berupa informasi pinjaman. Pelaku mengancam akan menyebarkan data nasabah apabila BSI tidak membayar tebusan. Tetapi Corporate Secretary BSI Gunawan A Hartoyo mengaku data para nasabah aman. Data Kependudukan dan Catatan Sipil (Dukcapil) pun mengalami kebocoran data di forum hacker Breach Forums berupa 337 juta. Terakhir akun Youtube DPR mengalami peretasan berupa gambar tulisan "slot baris"(Suharno, 2023).

Kasus kejahatan siber bukan saja berdampak pada kerugian finansial atau keuangan saja tetapi ancaman kejahatan pemilu. Kasus pada pemilu 2019, Komisi Pemilihan Umum (KPU) mengalami serangan *denial of service* (Ddos). Jenis kejahatan ini membuat server KPU *down* dampaknya adanya upaya peretasan untuk menyerang sistem informasi penghitungan (situng) untuk mengubah angka hasil penghitungan. KPU memiliki situng dengan sistem tertutup dan tidak tersambung dalam jaringan internet. Menurut ahli digital forensik Ruby Alamsyah, data penghitungan dilakukan secara manual berdasarkan hasil pemindahan surat C1 walaupun serangan ini tidak ada efeknya.(CNN Indonesia). Memasuki pemilu serentak 2024 ini, serangan siber termasuk dalam kategori sosial yang artinya berita hoax politik ataupun ujaran kebencian antar kubu calon presiden makin marak memenuhi ruang digital. Laporan pemetaan hoaks edisi Januari sampai dengan Maret 2023 dari Marfindo, hoax politik menempati urutan teratas (Dwi, 2023). Kontens Hoax akan selalu menyerang isu SARA berpotensi konflik di masyarakat di dunia digital maupun dunia nyata.

Kasus kejahatan yang dikemukakan di atas termasuk dalam kejahatan berupa serangan siber. Istilah serangan siber menurut Murti (2005) serangan siber atau

E-ISSN : 2988-5485 (online)

cyber crime merupakan sebuah istilah yang secara luas untuk menggambarkan tindak kejahatan dengan menggunakan media komputer atau internet. Pendapat lain tentang serangan siber dikemukakan oleh Gregory (2015), serangan siber merupakan bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung dengan internet.

Melalui Peraturan Komisi Pemilihan Umum (PKPU) Nomor 5 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum, untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan,dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya di lingkungan Komisi Pemilihan Umum. KPU juga menetapkan 2 (dua) Keputusan Komisi Pemilihan Umum sebagai pantuan PKPU Nomor 5/2021. Pertama, melalui Keputusan Komisi Pemilihan Umum Nomor 12/TIK.03/14/2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum Tahun 2021-2025. Kedua, Keputusan Komisi Pemilihan Umum Nomor 13/TIK.03/14/2022 tentang Peta Rancangan Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum Tahun 2021-2025.

Badan Siber dan Sandi Negara (BSSN) memiliki peran dalam tata kelola keamanan siber di Indonesia (Chusnul, 2019). Pelaksanaan siber Indonesia dilakukan melalui kerjasama bilateral dan multilateral. Keberadaan BSSN sebagai lembaga untuk mengkoordinasikan tugas-tugas lembaga dalam menangani dampak dari serangan siber yang begitu luas. Dampaknya bukan hanya pada masalah kerugian perekonomian saja tetapi hak individu pada ketuhanan dan kedaulatan negara maka pembangunan pertahanan dan keamanan siber adalah suatu kebutuhan untuk menjaga keamanan nasional di Indonesia (Catra, 2016).

Dengan berbagai kasus serangan siber, maka diperlukan suatu tata kelola keamanan siber yang sangat memadai. Serangan siber atau istilahnya *an attack from the weakest point of entry* merupakan betapa sukarnya mengatribusikan hackers, strategi dan motif yang dapat menimbulkan kerugian. Dalam artikel Iskandar (2019) membahas tata kelola keamanan siber di Singapura tentang fungsi penting agensi keamanan siber yang dimiliki oleh Singapura dan Undang-Undang yang mengatur. Dalam tulisan bertujuan membahas tentang bagaimana mengelola keamanan siber dalam menghadapi ancaman siber pada kejahatan siber pemilu.

B. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian secara kualitatif melalui teknik pengumpulan data *literature review* atau studi kepustakaan. Dalam studi kepustakaan, penulis menggunakan data yang berasal dari materi *webinar,* buku, jurnal ilmiah, regulasi peraturan dan artikel berita di media *online* pada pemilu tahun 2019 dan 2024.

C. PEMBAHASAN

Ancaman Serangan Siber Pemilu

Serangan siber pemilu di Indonesia dilakukan oleh oknum dengan memanfaatkan media komputer yang terhubung dengan jaringan internet. Melalui Undangan Forum Koordinasi dan Sinkronisasi (FKS) dari tindak lanjut Surat Kementerian Koordinator Bidang Politik, Hukum dan Keamanan Republik Nomor B-2660 perihal Permohonan Mengundang Perwakilan Pejabat KPU pada acara forum koordinasi dan Sinkronisasi (FKS) dalam menjalankan tugas dan fungsi koordinasi, sinkronisasi dan pengendalian (Korsidal). Tema dalam pertemuan yang dilaksanakan secara *daring* dan *luring* yaitu Koordinasi dan Sinkronisasi dalam rangka meningkatkan keamanan siber guna menghadapi pemilu tahun 2024.

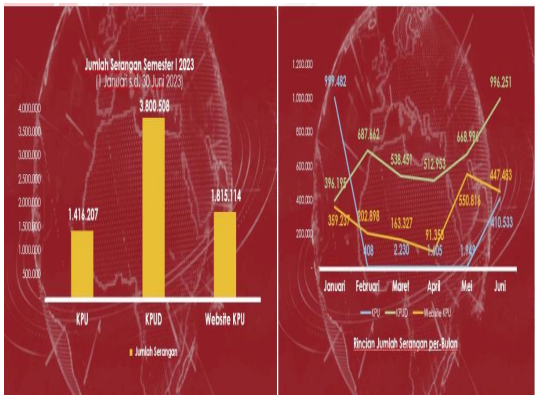
Badan Intelijen Negara (BIN) memiliki tugas dan fungsi yang tertuang dalam undang-undang nomor 17 Tahun 2021 Tentang Intelijen Negara. BIN memiliki

E-ISSN : 2988-5485 (online)

tugas dan tanggung jawab untuk melakukan upaya pekerjaan, kegiatan dan tindakan untuk mendeteksi dini dan peringatan dini dalam rangka pencegahan, penanganan dan penanggulangan terhadap ancaman yang mungkin timbul dan mengancam kepentingan dan keamanan nasional terkhusus dalam bidang intelijen siber. Deputi – VI BIN Bidang Intelijen Siber Direktorat Analisis dan Forensik telah mengemukakan 3 (tiga) jenis ancaman serangan siber pemilu 2024 yaitu :

1) Infrastruktur Jaringan
2) *Website* KPU yang ada di KPU, KPU Provinsi dan KPU Kabupaten/kota serta aplikasi tahapan pemilu.
3) Penyebaran Konten negatif yang ada di media sosial dan media *online* bentuknya seperti provokasi, hoax, *hate speech,* fitnah dan propaganda.

BIN merilis data serangan siber dengan KPU sebagai target utama selama semester I Tahun 2023 (1 Januari – 30 Juni 2023) dalam gambar di bawah ini :



Gambar 1.
Serangan Siber Kepada KPU pada Semester I Tahun 2023
Sumber : Threat Intelligence BIN, 2023

Data yang dirilis oleh BIN tentang serangan siber kepada KPU sepanjang semester I Tahun 2023 (1 Januari hingga 30 Juni 2023). Website atau laman KPU Daerah (KPU Provinsi/KPU Kabupaten/Kota) berada pada angka serangan sebesar 3.800.508 dan menempati peringkat pertama dibandingkan dengan website KPU RI berada peringkat kedua dengan serangan berjumlah 1.815.114. Urutan ketiga adalah sistem informasi yang dimiliki oleh KPU dengan jumlah serangan berjumlah 1.416.207. *Website* KPU menjadi sasaran serangan karena di masa tahapan pemilu, KPU selalu menyampaikan informasi dan berita seputaran tahapan pemilu serentak 2024.

Berdasarkan data jenis serangan siber yang dirilis oleh BIN, jenis serangan *MySQL Login Bruteforce* menempati urutan pertama dengan angka sebesar 520.669 dan disusul urutan kedua *Telnet Default Credentials* sebesar 461.938, peringkat ketiga Zivi PR115-204 *web camera* sebesar 8.614, Dasan GPN Remote Code Execution sebesar 1.598, Malware Trojan Andromeda sebesar 1.301, Malware Stealer Gozi sebesar 515, Eir D1000 Modem CWMP Command Injection sebesar 568 dan Multiple CCT Vendors Remote code execution sebesar 320.

Jenis serangan terbesar adalah MySQL Login brute force dengan tampilan seperti dibawah ini :

Gambar 2.
Tampilan MySQL Login brute force
Sumber : Threat Intelligence BIN, 2023

Jenis serangan ini menyerang peretasan password MySQL dengan menggunakan algoritma brute force. Serangan brute force (Eka, 2011) adalah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci uang mungkin. Brute force attack adalah teknik menjebol kode rahasia dengan deskripsi sebuah teks

E-ISSN : 2988-5485 (online)

yang telah terenkripsi dengan mencoba sebuah kunci yang ada.

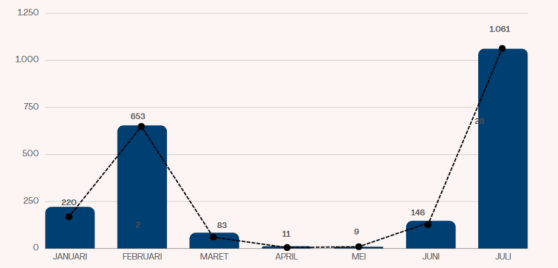
Motif serangan siber melalui tren transformasi spionase dan sabotase melalui ruang siber, BIN mengemukakan terdapat 4 (empat) motif serangan yaitu :

1. Pengumpulan Data
2. Mendapatkan keuntungan uang
3. Menyerang/mendiskreditkan
4. Sabotase pelaksanaan pemilu

Dari keempat motif serangan tersebut, pada motif keempat sabotase pelaksanaan pemilu merupakan dampak dari motif serangan kepada KPU. Sebagai penyelenggara pemilu jika sistem KPU diserang tentu akan menjadi permasalahan di masyarakat tentang kredibilitas KPU dalam mengatasi serangan siber. Seperti contoh pada tahapan penghitungan suara, apabila hasil penghitungan suara diserang maka berdampak pada tidak kepercayaan kepada KPU dalam menjalankan pemilu.

Kebocoran data dapat terjadi karena adanya eksploitasi kerentanan keamanan pada sistem hingga disebabkan infeksi malware. Setidaknya ada 5 (lima) faktor penyebab insiden serangan siber yaitu 1). Kerentanan keamanan pada sistem aplikasi dan infrastruktur jaringan; 2). Sistem elektronik dibangun tanpa pertimbangan keamanan siber dan hanya tambal sulam; 3). Cyber security awareness pejabat atau pegawai pemerintah dinilai masih rendah, 4). Banyaknya perangkat *endpoint* yang terinfeksi malware stealer dan 5). Tata kelola keamanan siber khususnya di instansi pemerintah masih rendah karena sebagian besar tidak memiliki SDM berkualitas dalam siber.

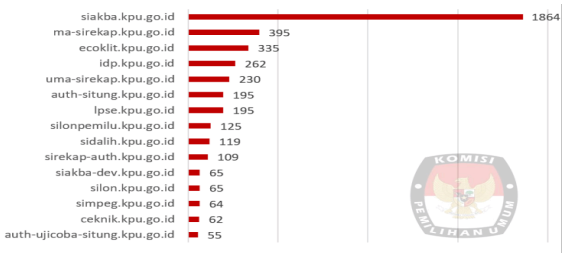
Banyaknya perangkat *endpoint* (Komputer dan Laptop) yang terinfeksi malware stealer menjadi penyebab utama serangan siber kebocoran data. BIN telah merilis hasil 1.839 kredensial tentang kebocoran data milik KPU periode Januari sampai dengan Juli 2023 seperti pada gambar diagram di bawah ini :



Gambar 3.
Kebocoran Data Kredensial Milik KPU RI periode Januari – Juli 2023
Sumber : Threat Intelligence BIN, 2023

Dengan total 1.839 kredensial berasal dari 157 sistem informasi atau aplikasi milik KPU seperti siakba.kpu.go.id, ma-sirekap.kpu.go.id, idp.kpu.go.id, auth-situng.kpu.go.id, uma-sirekap.go.id dan lain-lain. Serangan perangkat keras laptop dan komputer milik pegawai KPU merupakan jenis Malware Stealer Readline Stealer, raccoon, AZORULT. KPU memiliki website aplikasi untuk mendukung pelaksanaan tugas pemilu dan pilkada serentak.

Dalam pemilu serentak 2019, KPU mengalami serangan siber dengan total 25.859.836 serangan. Adapun tipe serangan yaitu :1. *HTTP Parser Attack, 2. Abuse of functionality, 3. Detection Evasion, 4. Injection Attempt, 5. Information Leakage, 6. Forced Browsing, 7. Non-browser client, 8. Buffer overflow, 9 Vulnerability scan*, 10. Session Hijacking.

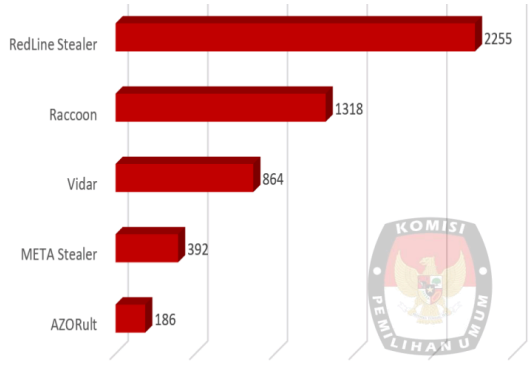


Gambar 4.
Website Aplikasi KPU mengalami kebocoran data periode Januari – Agustus 2023
Sumber : Threat Intelligence BIN, 2023

E-ISSN : 2988-5485 (online)

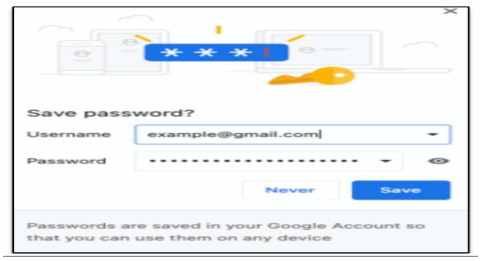
BIN kembali merilis website aplikasi KPU yang paling banyak mengalami kebocoran data kredensial. Hasilnya Siakba KPU mengalami kebocoran data sebanyak 1.864 dengan peringkat teratas pada periode Januari – agustus 2023

Serangan siber penyebab kebocoran data KPU, BIN menyatakan jika terdapat jenis malware stealer yang menyebabkan kebocoran data kredensial KPU seperti dalam gambar di bawah ini :



Gambar 5. Malware Stealer penyebab kebocoran data kredensial KPU
Sumber : Threat Intelligence BIN, 2023

Dari gambar diatas readline stealer menempati urutan teratas sebesar 2255 penyebab kebocoran data KPU. Malware Stealer sendiri merupakan jenis perangkat lunak berbahaya yang dirancang untuk mencuri informasi pribadi atau data sensitif dari komputer korban berupa data *username* dan *password.* Contoh malware berhasil menginfeksi perangkat pencurian data username dan password di aplikasi browser seperti di bawah ini :



Gambar. 6.
Browser terinfeksi malware
Sumber : Threat Intelligence BIN, 2023

Penyebab infeksi malware stealer menurut BIN, adanya kurang kesadaran keamanan siber. Ketika browsing pengguna tidak dapat mendeteksi adanya ancaman siber melalui email masuk padahal itu adalah email phising, selain itu juga adanya iklan yang mengandung malware atau malvertising, drive by download. Dampaknya kelemahan keamanan berakibat perangkat lunak menjadi usang, konfigurasi keamanan lemah dan penggunaan antivirus yang tidak efektif. Dampak malware stealer setidaknya ada 3 (tiga) dampak yaitu :

1. Kehilangan data sensitif berupa data personal, rahasia negara, dan informasi keuangan;
2. Potensi penyalahgunaan data berupa penipuan dan spionase;
3. Keamanan nasional berupa kehilangan kepercayaan publik dan terciptanya situasi yang tidak kondusif di masyarakat.

Berdasarkan laporan *National Cyber Security Indeks (*NCSI) skor indeks keamanan siber Indonesia sebesar 28,96 poin dari 100 pada tahun 2022. Angka ini menempatkan Indonesia di peringkat ke-3 terendah di antara negara-negara G20. (Mutia, 2022). BSSN memiliki peran dalam menjalin koordinasi dan kerjasama antar institusi dan pemangku kepentingan di bidang siber secara nasional maupun internasional. Melalui Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2021 tentang Perubahan atas peraturan badan siber dan sandi Negara Nomor 5 Tahun 2020 tentang rencana strategis badan siber dan sandi negara tahun 2020-2024. BSSN memiliki visi sebagai berikut "Badan siber dan sandi negara yang andal, profesional, inovatif dan berintegritas dalam pelayanan kepada presiden dan wakil presiden untuk mewujudkan visi misi Presiden dan wakil presiden Indonesia maju yang berdaulat mandiri dan berkepentingan berdasarkan gotong royong.

E-ISSN : 2988-5485 (online)

Pencegahan dan Mengatasi Ancaman Kejahatan Siber Pemilu

BSSN berperan dalam pencegahan dan mengatasi ancaman kejahatan siber pemilu (Carley, 2020) yaitu :

1. *Cybersecurity (D21)*

Fokus pada serangan yang dilakukan pada dan melalui infrastruktur dunia siber yang dimaksudkan untuk mengganggu teknologi, mencuri atau menghancurkan informasi, atau mencuri identitas atau uang. Contoh : *cyber breach, data compromise, malware detection. denial-of-service attack protection. Proses : identification, protection, detection, response, recover.*

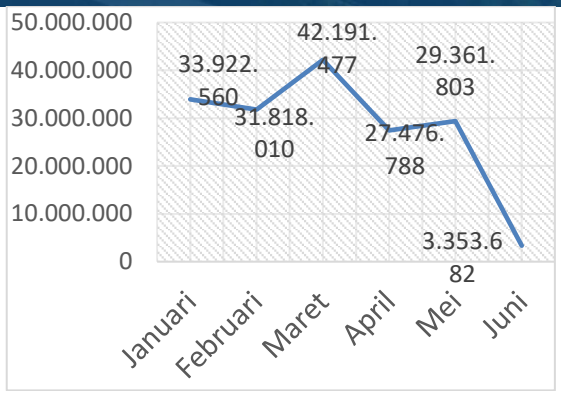
2. *Sosial cybersecurity (D22)*

Fokus pada aktivitas yang ditujukan untuk mempengaruhi atau memanipulasi individu, kelompok, atau komunitas, khususnya aktivitas yang memiliki konsekuensi besar bagi kelompok sosial, organisasi, dan negara. Contoh : *Spread of disinformation, information diffusion, extremist recruiting, political polarization, manipulation of extremist funding. Proses : Social Cyber Forensic, Information Maneuvers, Motive Identification, Diffusion, Impact Measurement, Mitigation*

3. *Signal and Cryptography (D23)*

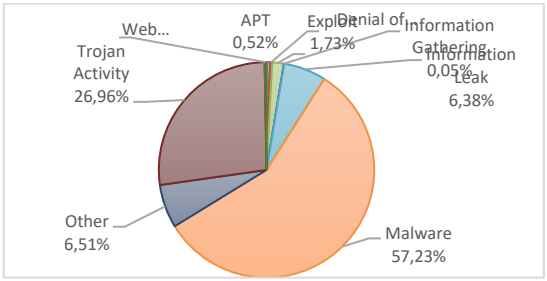
Fokus pada serangan yang ditujukan dalam bentuk surveillance (penyadapan) atau penyalahgunaan data strategis sehingga berpotensi pada terjadi kebocoran data. Contoh *: Active surveillance, Bugging, data compromise, Passive surveillance, Signal monitoring*. Proses : Kontra Penginderaan , Jammer, KMS *(Key Management System)*

BSSN merilis progres pelaksanaan pengamanan siber pemilu 2024. Dalam tren anomali trafik keamanan siber nasional tercatat terdapat 168.124.320 anomali trafik periode 1 Januari – 3 Juni 2023, dengan gambar di bawah ini :



Gambar. 7
Tren Anomali Trafik 2023
Sumber : BSSN, 2023

Gambar grafik diatas menunjukkan tercatat 168.124.320 trafik selama semester pertama tahun 2023. Top 3 jenis anomali trafik menurut BSSN yaitu 57,23 % Malware activity, 26,96 % trojan activity dan 6,38% information leak. Sementara tren klarifikasi anomali lebih detail pada gambar di bawah ini :



Gambar 8.
Trend klasifikasi anomali grafik
Sumber : BSSN, 2023

Pada gambar klasifikasi grafik merupakan bentuk serangan secara teknis maka BSSN berperan dalam pengaman siber pemilu serentak 2024 melalui tim operasi pengamanan pemilu 2024. Tim operasi ini bertugas melaksanakan operasi pengamanan siber pada penyelenggaraan pemilu sejak tahapan pendaftaran peserta pemilu 2024 tepatnya bulan agustus 2023 hingga selesai menjabat pada penyelesaian sengketa pemilu 2024 yaitu oktober 2024. Tim operasi didukung oleh 6 (enam) teknis tim yaitu :

1. Tim information technology security assessment

E-ISSN : 2988-5485 (online)

2. Tim deteksi atau monitoring
3. Tim cyber threat intelligence dan therea hunting
4. Tim Pengamanan persandian
5. Tim Digital forensik and incident response
6. Tim pengendalian informasi

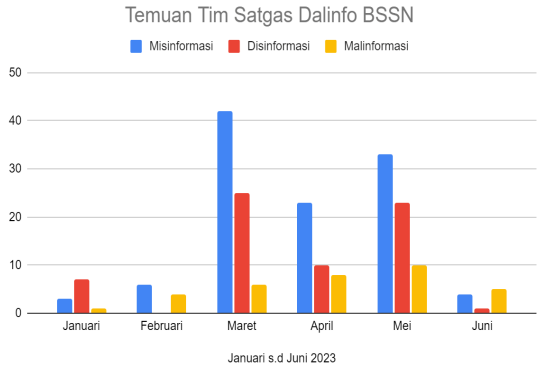
Dalam mengawal suksesnya gerangan pemilu serentak tahun 2024, BSSN melaksanakan berbagai kegiatan yaitu :

1. Monitoring dan analisis isu aktual pemilu di media online dan media sosial
2. Edukasi dan literasi terhadap ancaman siber bersifat sosial
3. Verifikasi cepat dengan memastikan kebenaran informasi dari berbagai sumber
4. Pengertian narasi dan pengaruh informasi untuk keberhasilan kelancaran dan kesuksesan pelaksanaan pemilu
5. Pemberian rekomendasi pendindakan dan pembloklirang oleh piha brwenang.

Dalam pelaksanaan operasi, BSSN membentuk 4 (empat) tim operasi yaitu :

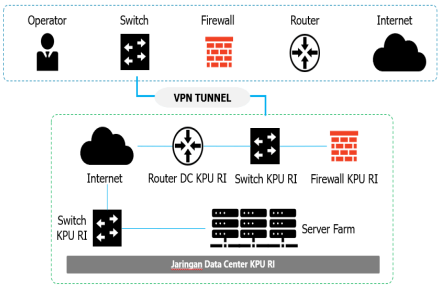
1. Tim operasi keamanan siber
   Melaksanakan monitoring,identifikasi proteksi penanggulangan dan pemulihan ke seluruh infrasutir dan aset siber.
2. Tim operasi pengendalian informasi
   Melaksanakan monitoring dan analisis media sosial, media online forum data breach terkait isu sosio kultural serta melakukan kotoran dan penguatan narasi
3. Tim operasi sandi
   Melaksanakan penerapan fungsi kriptografi, kontranpemhmideraan, pengamaann signal dan gelar jaring komunikasi yang aman.
4. Tim komunikasi publik
   Melaksanakan pelaporan dan penyampaian informasi terkini satgas peams bersandi pemilu 2024 BSSN Kepada masyarakat dan media massa.

Hasil temuan lain dari tim Dalinfo Pemilu, berupa temuan gangguan informasi pemilu per Januari hingga Juni 2023. Gangguan informasi terbanyak merupakan media informasi dan gangguan informasi dalam kategori konten yang menyesatkan. Seperti dalam gambar di bawah ini :



Gambar.9
Temuan Tim Satgas Dalinfo BSSN
Sumber : BSSN, 2023

Dalam hal pengamanan siber, Wakit (2023) KPU menerapkan pengamanan siber dengan beberapa cara yaitu : 1).Pengembangan aplikasi dan pengembangan sistem; 2).Pengamanan data center dan jaringan; 3).Pengamanan Pengoperasian; 4).Pengamanan fisik dan 5).Audit. Untuk itu dalam pelayanan publik tugas kepemiluan yang terkoneksi dalam jaringan internet. Koneksi ini merupakan celah terjadinya serangan siber, maka KPU mendesain topologi keamanan siber sebagai berikut :

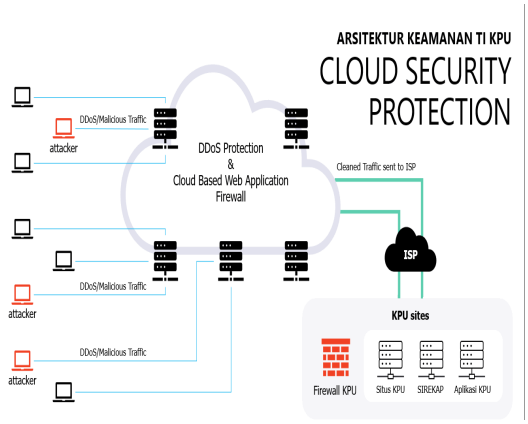


Gambar 10.
Jaringan Internet KPU Kabupaten/Kota
Sumber : KPU, 2023

Secara komplek, KPU mendesain keamanan Teknologi Informasi melalui *Cloud Security Protection.* Menurut Bagus (2023) *Cloud Security* adalah perlindungan

E-ISSN : 2988-5485 (online)

data, aplikasi atau infrastruktur yang terlibat dalam komputasi *cloud.* Adapun desain yang diterapkan oleh KPU sebagai berikut :



Gambar 11.
Desain *Cloud Security Protection* KPU
Sumber : KPU, 2023

D. PENUTUP DAN REKOMENDASI

KPU senantiasa menjadi korban kejahatan pemilu dimulai dari serangan siber berbasis teknis, sosial dan transmisi. Melalui tata kelola kelembagaan yang baik melalui peraturan yang dibuat KPU dan melakukan kolaborasi dengan kementerian terkait dalam upaya mencegah dan mengatasi ancaman pemilu serentak 2024. Kewenangan KPU dalam menetapkan regulasi untuk sebagai dasar tata kelola pemerintahan yang baik. Penerapan ini dapat dilakukan dari tingkat pusat hingga daerah bahkan di tingkat badan *ad hoc.* Rekomendasi dari tulisan ini adalah Penerapan CSIRT setiap lembaga negara untuk mendukung dalam keamanan siber dan pencegahan serta mengatasi ancaman siber pemilu dan pilkada.

REFERENSI

Bagus, W,S. (2023) Cloud Security adalah:pengertian, keuntungan dan penerapannya dalam https://digitalsolusigrup.co.id/cloud-security-adalah/ diakses pada tanggal 3 September 2023 pukul 18:42 WIB

BSSN, (2023) BSSN Dan Kemenkominfo Sepakat Tangkal Serangan Siber Sosial Dalam Rangka Pengamanan Ruang Siber Pada Pemilu 2024 dalam https://www.bssn.go.id/bssn-dan-kemenkominfo diakses pada tanggal 3 September 2023 pukul 18:42 WIB

Carley, K. M.(2020.) "Social Cybersecurity: An Emerging Science," Computational and mathematical organization theory (26:4);

CATRA. "Dari Desk Cyberspace Nasional Menuju Badan Cyber Nasional". Majalah Setjen Wantannas, Edisi VI September 2016.

Chusnul, C,H (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara;

CNN Indonesia, (2019). Ahli Ungkap KPU Alami Serangan Siber Saat Pencoblosan. https://www.cnnindonesia.com/teknologi/20190527152001-185-398784/ahli-ungkap-kpu-alami-serangan-siber-saat-hari-pencoblosan diakses pada tanggal 3 September 2023 pukul 18:42 WIB

Dal.(2020) Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologilengkap-91-juta-akun-tokopedia-bocor-dan-dijual. Diakses tanggal 7 September 2023;.

DKPP,(2023) DKPP Periksa KPU Trenggalek Terkait Kebocoran Data Pribadi Calon PPS – DKPP RI – Dewan Kehormatan Penyelenggara Pemilu Republik Indonesia Diakses tanggal 7 September 2023;.

Dwi, A,P, (2023) Serangan Siber, Ancaman Serius Pemilu 2024. RRI - Serangan Siber, Ancaman Serius Pemilu

E-ISSN : 2988-5485 (online)

2024, diakses pada tanggal 6 September 2023 pukul 18:52 WIB.

Gregory, Thomas HA, (2005) "Ketenaran Cybercrime di Indonesia", Makalah STIMIK Perbanas 2005 yang dipublikasikan diakses pada 19 Desember 2008;

Iskandar, P,K.(2019).Belajar Dari Tata Kelola Keamanan Siber Singapore,Case Study Series#44 Januari 2019; Center For Digital Society, Yogyakarta;

Keputusan Menteri Politik Hukum dan Keamanan Nomor 125 Tahun 2022

Krisnaldi Eka Pramudita (2011) "Brute Force Attack dan Penerapannya pada Password Cracking". Makalah IF3051 Strategi Algoritma. ITB. Bandung;

Murti, Hari. (2005) Cybercrime." Dinamik, vol. 10, no. 1,.

Mutia, (2022) https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia diakses pada tanggal 6 September 2023 pukul 18:52 WIB.

Nyoman Amie Sandrawati. (2022). Antisipasi Cybercrime Dan Kesenjangan Digital Dalam Penerapan Tik Di Kpu. Electoral Governance Jurnal Tata Kelola Pemilu Indonesia, 3(2), 232-257. https://doi.org/10.46874/tkp.v3i2.655

Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021;

Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2021;

Peraturan Komisi Pemilihan Umum Nomor 5 Tahun 2021;

Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2018;

Pradesa, H.A., Agustina, I., & Wijayati, I., Y. (2023). Pelaksanaan Review Kerangka Kerja Manajemen Risiko Pada Lembaga Administrasi Negara Republik Indonesia. *Aksiologiya: Jurnal Pengabdian Kepada Masyarakat*, 7 (3), 330 – 343.

Pradesa, H.A.; Purba, C..O.; Priatna, R. (2021). Menilai risiko dari organisasi yang bertransformasi: pelajaran terbaik untuk penguatan akuntabilitas pendidikan tinggi di Indonesia**.** Jurnal Akuntabilitas Manajemen Pendidikan, 9 (2), p. 146-158, DOI:https://doi.org/10.21831/jamp.v9i2.40104.

RRI, (2023) https://www.rri.go.id/papua-barat/editorial/1665/serangan-siber-ancaman-serius-pemilu-2024

Suharno, (2023) Deretan Kejahatan Siber yang terjadi di Indonesia Tahun 2023. Https://www.Selular.id/2023/09/deretan-kejahatan-siber-yang-terjadi-di-indonesia-tahun-2023/2/ diakses tanggal 03 September 2023 pukul 16:44 WIB

Uli.(2021). Kronologi Grab Toko Tipu 980 Orang dan Rugikan Rp 17 M. https://www.cnnindonesia.com/ekonomi/20210115135836-92-594181/kronologi-grabtoko-tipu-980-orang-dan-rugikan-rp17-m. Diakses tanggal 7 September 2023;