

BAB II

DINAMIKA KEAMANAN SIBER NASIONAL DAN INSIDEN *DEFACEMENT* SITUS PUSMANAS

2.1. BSSN sebagai Lembaga Keamanan Siber Nasional Indonesia

2.1.1. Sejarah Pembentukan Badan Siber dan Sandi Negara

Perkembangan teknologi informasi dan komunikasi di Indonesia telah mendorong perubahan dalam berbagai aspek kehidupan, termasuk dalam penyelenggaraan pemerintahan, pelayanan publik, perekonomian, serta komunikasi masyarakat. Perkembangan tersebut pada saat yang sama meningkatkan ketergantungan negara terhadap sistem elektronik dan infrastruktur digital. Ketergantungan tersebut kemudian menimbulkan kebutuhan terhadap sistem keamanan yang mampu melindungi informasi dan sistem elektronik dari berbagai bentuk ancaman. Pada awalnya, pengamanan informasi negara di Indonesia lebih banyak berkaitan dengan bidang persandian yang menjadi bagian penting dalam menjaga kerahasiaan informasi strategis pemerintah. Seiring dengan berkembangnya penggunaan teknologi digital dan meningkatnya kompleksitas ancaman di ruang siber, kebutuhan tersebut berkembang tidak lagi terbatas pada perlindungan informasi melalui persandian, tetapi juga mencakup perlindungan terhadap jaringan, sistem elektronik, data, serta infrastruktur digital secara lebih luas. Kondisi tersebut kemudian mendorong pemerintah Indonesia untuk membangun kelembagaan yang secara khusus dapat menangani persoalan

keamanan siber secara lebih terintegrasi. (Badan Siber dan Sandi Negara [BSSN], 2022).

Sebelum terbentuknya Badan Siber dan Sandi Negara (BSSN), fungsi yang berkaitan dengan persandian negara dijalankan oleh Lembaga Sandi Negara (Lemsaneg). Lembaga tersebut memiliki peran dalam penyelenggaraan persandian negara sebagai bagian dari upaya menjaga keamanan informasi. Namun, perkembangan ancaman siber menunjukkan bahwa pengamanan informasi melalui fungsi persandian saja tidak lagi cukup untuk menghadapi karakter ancaman digital yang semakin kompleks. Serangan terhadap sistem informasi dapat dilakukan melalui berbagai metode, seperti peretasan, malware, pencurian data, serangan terhadap jaringan, hingga gangguan terhadap sistem elektronik milik pemerintah. Perubahan karakter ancaman tersebut menyebabkan kebutuhan terhadap suatu lembaga yang tidak hanya berfokus pada persandian, tetapi juga memiliki kapasitas untuk melakukan identifikasi, deteksi, perlindungan, penanggulangan, dan pemulihan terhadap berbagai ancaman siber. Oleh karena itu, pemerintah mulai melakukan penguatan kelembagaan keamanan siber melalui pembentukan institusi yang memiliki mandat lebih luas dalam mengelola keamanan siber nasional (BSSN, 2022).

Upaya tersebut diwujudkan melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara. Melalui peraturan tersebut, pemerintah membentuk BSSN sebagai lembaga yang mengintegrasikan fungsi keamanan siber dan persandian dalam satu

kelembagaan. Pembentukan BSSN menjadi langkah penting dalam perkembangan kebijakan keamanan siber Indonesia karena menunjukkan adanya perubahan pendekatan pemerintah dari pengamanan informasi yang sebelumnya lebih berorientasi pada persandian menuju pendekatan keamanan siber yang lebih komprehensif. BSSN kemudian ditempatkan sebagai lembaga yang memiliki tanggung jawab dalam penyelenggaraan keamanan siber nasional, sehingga keberadaannya diharapkan dapat memperkuat kemampuan negara dalam menghadapi ancaman yang muncul dari perkembangan teknologi digital. Pembentukan tersebut juga menunjukkan bahwa keamanan ruang siber mulai dipandang sebagai bagian penting dari kepentingan nasional yang membutuhkan koordinasi dan penanganan secara kelembagaan. Dasar pembentukan tersebut kemudian mengalami perubahan melalui Peraturan Presiden Nomor 133 Tahun 2017 yang mengubah beberapa ketentuan dalam Perpres Nomor 53 Tahun 2017 (Republik Indonesia, 2017).

Perkembangan kelembagaan BSSN kemudian mengalami penyesuaian kembali melalui Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Peraturan tersebut mencabut Perpres Nomor 53 Tahun 2017 sebagaimana telah diubah dengan Perpres Nomor 133 Tahun 2017 dan menjadi dasar hukum BSSN yang berlaku dalam penyelenggaraan keamanan siber dan persandian. Perubahan tersebut menunjukkan adanya proses penguatan dan penyesuaian kelembagaan pemerintah terhadap perkembangan kebutuhan keamanan siber nasional.

Melalui Perpres Nomor 28 Tahun 2021, BSSN ditegaskan sebagai lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden serta memiliki tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan. Dengan demikian, perkembangan BSSN dapat dipahami sebagai bagian dari proses institusionalisasi keamanan siber di Indonesia, yaitu proses ketika keamanan ruang digital tidak lagi dipandang semata-mata sebagai persoalan teknis, tetapi menjadi bagian dari tata kelola pemerintahan dan kepentingan nasional.

Pembentukan dan perkembangan BSSN juga menjadi semakin relevan seiring dengan meningkatnya penggunaan sistem elektronik dalam penyelenggaraan pemerintahan Indonesia. Sistem digital yang digunakan oleh lembaga negara memiliki peran penting dalam penyediaan informasi, pelayanan publik, komunikasi pemerintahan, serta penyimpanan dan pengelolaan berbagai informasi. Kondisi tersebut menyebabkan gangguan terhadap sistem elektronik pemerintah dapat memberikan dampak yang lebih luas dibandingkan gangguan terhadap sistem milik organisasi biasa. Dalam konteks tersebut, keberadaan BSSN menjadi penting karena lembaga ini tidak hanya berkaitan dengan perlindungan informasi, tetapi juga berperan dalam membangun kemampuan negara untuk menghadapi ancaman siber yang dapat mengganggu sistem elektronik pemerintah. Hal tersebut menjadi semakin relevan dalam penelitian ini karena salah satu sistem yang berada dalam lingkungan BSSN, yaitu Pusat Malware Nasional

(Pusmanas), pernah mengalami serangan web *defacement* pada tahun 2021. Kasus tersebut menjadi penting untuk dikaji karena serangan terjadi terhadap institusi yang secara langsung memiliki mandat dalam bidang keamanan siber nasional. Oleh karena itu, sejarah pembentukan BSSN menjadi landasan untuk memahami kedudukan, peran, serta tanggung jawab BSSN sebelum pembahasan lebih lanjut mengenai profil, tugas dan fungsi, kewenangan, serta kebijakan keamanan siber pemerintah Indonesia pada bagian berikutnya.

2.1.2. Profil dan Kedudukan Badan Siber dan Sandi Negara (BSSN)

Badan Siber dan Sandi Negara (BSSN) merupakan lembaga pemerintah yang memiliki peran strategis dalam penyelenggaraan keamanan siber nasional Indonesia. Pembentukan BSSN merupakan bagian dari upaya pemerintah untuk membangun kelembagaan yang secara khusus menangani keamanan siber dan persandian dalam menghadapi perkembangan ancaman di ruang digital. Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara, BSSN merupakan lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden. Kedudukan tersebut menunjukkan bahwa keamanan siber ditempatkan sebagai salah satu bagian penting dalam penyelenggaraan pemerintahan dan memiliki keterkaitan langsung dengan kepentingan nasional. Sebagai lembaga yang bertanggung jawab kepada Presiden, BSSN memiliki posisi strategis dalam membantu pemerintah membangun sistem

keamanan siber yang mampu melindungi kepentingan nasional dari berbagai bentuk ancaman digital (Republik Indonesia, 2021).

Secara kelembagaan, BSSN memiliki cakupan tanggung jawab yang tidak hanya terbatas pada perlindungan terhadap sistem digital milik pemerintah, tetapi juga mencakup penyelenggaraan keamanan siber secara lebih luas. Perkembangan teknologi digital menyebabkan berbagai sektor kehidupan semakin bergantung pada sistem elektronik, mulai dari pemerintahan, pelayanan publik, keuangan, kesehatan, pendidikan, hingga sektor strategis lainnya. Kondisi tersebut menyebabkan gangguan terhadap sistem elektronik dapat memberikan dampak yang lebih luas terhadap masyarakat dan kepentingan negara. Oleh karena itu, keberadaan BSSN menjadi penting sebagai institusi yang memiliki mandat dalam membangun dan memperkuat keamanan siber nasional. Posisi tersebut menempatkan BSSN sebagai salah satu aktor utama dalam upaya pemerintah menghadapi ancaman siber yang semakin beragam dan kompleks (BSSN, 2022).

Dalam menjalankan kedudukannya sebagai lembaga pemerintah di bidang keamanan siber dan persandian, BSSN memiliki hubungan yang erat dengan berbagai kementerian, lembaga pemerintah, pemerintah daerah, serta penyelenggara sistem elektronik lainnya. Hal tersebut disebabkan oleh karakter ancaman siber yang bersifat lintas sektor dan tidak terbatas pada satu institusi tertentu. Serangan terhadap suatu sistem dapat memiliki keterkaitan dengan sistem atau jaringan yang dikelola oleh institusi lain sehingga penanganannya membutuhkan koordinasi dan pertukaran

informasi. Oleh karena itu, BSSN tidak hanya berperan sebagai lembaga yang melakukan pengamanan secara langsung, tetapi juga memiliki posisi sebagai salah satu pusat koordinasi dalam penyelenggaraan keamanan siber nasional. Kebutuhan terhadap koordinasi tersebut menjadi semakin penting karena sistem elektronik pemerintah memiliki tingkat ketergantungan yang tinggi terhadap jaringan dan infrastruktur digital (Republik Indonesia, 2021).

Kedudukan strategis BSSN juga dapat dilihat dari ruang lingkup keamanan yang menjadi tanggung jawabnya, yaitu keamanan siber dan persandian. Persandian berkaitan dengan upaya menjaga keamanan informasi melalui penerapan teknik dan sistem persandian, sedangkan keamanan siber memiliki cakupan yang lebih luas karena berkaitan dengan perlindungan ruang siber dari berbagai ancaman yang dapat mengganggu sistem elektronik, jaringan, maupun informasi. Penggabungan kedua bidang tersebut dalam satu institusi menunjukkan bahwa pemerintah memandang perlindungan informasi dan keamanan sistem digital sebagai dua aspek yang saling berkaitan. Dalam perkembangan lingkungan keamanan modern, informasi menjadi salah satu aset strategis sehingga upaya perlindungannya tidak hanya dilakukan melalui mekanisme teknis, tetapi juga melalui penguatan kelembagaan, sumber daya manusia, regulasi, dan koordinasi antaraktor (Republik Indonesia, 2021).

Sebagai lembaga yang memiliki kedudukan strategis dalam keamanan siber nasional, BSSN juga memiliki peran penting dalam menghadapi berbagai bentuk insiden keamanan siber yang terjadi pada sistem elektronik pemerintah. Salah satu contoh yang menunjukkan pentingnya posisi tersebut adalah insiden web *defacement* terhadap situs Pusat Malware Nasional (Pusmanas) pada tahun 2021. Pusmanas merupakan salah satu layanan yang dikembangkan oleh BSSN dan memiliki fungsi dalam identifikasi, analisis, dokumentasi, serta penyebaran informasi mengenai malware dan ancaman siber. Dengan demikian, serangan terhadap situs Pusmanas memiliki dimensi yang berbeda dibandingkan serangan terhadap situs biasa karena terjadi pada sistem yang berada dalam lingkungan lembaga yang memiliki tanggung jawab di bidang keamanan siber nasional. Kondisi tersebut menjadikan kasus Pusmanas relevan untuk melihat bagaimana posisi strategis BSSN diikuti dengan kemampuan dalam menjaga sistem yang berada di bawah pengelolaannya (BSSN, 2022).

Berdasarkan uraian tersebut, BSSN dapat dipahami sebagai lembaga pemerintah yang memiliki posisi strategis dalam struktur keamanan siber Indonesia. Kedudukannya yang berada di bawah dan bertanggung jawab kepada Presiden memberikan BSSN mandat kelembagaan untuk mendukung penyelenggaraan keamanan siber dan persandian secara nasional. Namun, kedudukan formal suatu lembaga tidak secara otomatis menunjukkan efektivitas pelaksanaan tugasnya. Kemampuan BSSN dalam menjalankan mandat tersebut juga dipengaruhi oleh kapasitas kelembagaan,

koordinasi antarinstansi, sumber daya, serta kemampuan dalam merespons ancaman dan insiden siber. Oleh karena itu, pemahaman mengenai profil dan kedudukan BSSN menjadi dasar untuk melihat tugas dan fungsi yang dimiliki lembaga tersebut serta bagaimana mandat tersebut diterapkan dalam menghadapi ancaman keamanan siber di Indonesia (Republik Indonesia, 2021).

2.1.3. Tugas Pokok dan Fungsi Badan Siber dan Sandi Negara (BSSN)

Badan Siber dan Sandi Negara (BSSN) memiliki tugas utama melaksanakan pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan. Tugas tersebut menunjukkan bahwa BSSN memiliki mandat yang luas dalam menjaga keamanan ruang siber nasional serta memastikan penyelenggaraan fungsi persandian negara dapat berjalan secara efektif. Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021, tugas BSSN tidak hanya berkaitan dengan penanganan serangan yang telah terjadi, tetapi juga mencakup berbagai upaya untuk membangun keamanan siber secara menyeluruh. Dengan demikian, tugas BSSN dapat dipahami sebagai bagian dari upaya negara dalam menciptakan kondisi ruang siber yang aman dan terlindungi dari berbagai bentuk ancaman yang dapat mengganggu kepentingan nasional (Republik Indonesia, 2021).

Dalam menjalankan tugas tersebut, BSSN memiliki fungsi yang mencakup perumusan dan penetapan kebijakan teknis di bidang keamanan siber dan sandi. Fungsi tersebut menjadi penting karena perkembangan

ancaman siber membutuhkan kebijakan yang mampu menyesuaikan diri dengan perubahan teknologi dan karakteristik serangan. Kebijakan yang dirumuskan oleh BSSN menjadi salah satu dasar dalam menentukan standar, mekanisme, serta langkah yang perlu dilakukan oleh berbagai pihak dalam menjaga keamanan sistem elektronik. Selain itu, BSSN juga memiliki fungsi dalam pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi, sehingga terdapat hubungan antara perumusan kebijakan dengan implementasinya di lapangan. Melalui fungsi tersebut, BSSN tidak hanya berperan sebagai pembuat kebijakan, tetapi juga memiliki tanggung jawab dalam memastikan kebijakan keamanan siber dapat diterapkan dalam penyelenggaraan keamanan siber nasional (Republik Indonesia, 2021).

Fungsi BSSN juga mencakup pelaksanaan pemantauan, identifikasi, deteksi, proteksi, penanggulangan, dan pemulihan terhadap berbagai ancaman keamanan siber. Tahapan tersebut menunjukkan bahwa pelaksanaan keamanan siber oleh BSSN memiliki karakter yang berkelanjutan, mulai dari sebelum terjadinya serangan hingga setelah suatu insiden berhasil ditangani. Pemantauan dan identifikasi dilakukan untuk mengetahui potensi ancaman serta kerentanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang, sedangkan deteksi bertujuan untuk mengetahui adanya aktivitas atau indikasi serangan terhadap sistem. Apabila ancaman telah teridentifikasi, tindakan proteksi diperlukan untuk mengurangi kemungkinan terjadinya gangguan terhadap sistem. Sementara itu, penanggulangan dan pemulihan dilakukan ketika suatu insiden telah

terjadi dengan tujuan membatasi dampak serangan dan mengembalikan sistem agar dapat berfungsi kembali. Rangkaian fungsi tersebut menunjukkan bahwa tanggung jawab BSSN mencakup keseluruhan siklus pengelolaan ancaman dan insiden keamanan siber (Republik Indonesia, 2021).

Selain fungsi yang berkaitan dengan pengelolaan ancaman, BSSN juga memiliki fungsi dalam pelaksanaan koordinasi dan dukungan terhadap penyelenggaraan keamanan siber nasional. Karakter ancaman siber yang bersifat lintas batas dan lintas sektor menyebabkan penanganannya tidak dapat dilakukan hanya oleh satu institusi. Sistem elektronik pemerintah, sektor strategis, serta berbagai penyelenggara sistem elektronik memiliki keterhubungan yang dapat menyebabkan suatu serangan memberikan dampak terhadap lebih dari satu pihak. Dalam kondisi tersebut, koordinasi menjadi bagian penting dalam memastikan informasi mengenai ancaman dan insiden dapat ditangani secara tepat. BSSN memiliki peran dalam membangun koordinasi dengan kementerian, lembaga, pemerintah daerah, serta pihak lain yang berkaitan dengan penyelenggaraan keamanan siber. Melalui koordinasi tersebut, penanganan ancaman siber dapat dilakukan secara lebih terintegrasi sehingga respons terhadap suatu insiden tidak berjalan secara terpisah antarinstansi (Republik Indonesia, 2021).

Dalam konteks penanganan insiden, fungsi BSSN memiliki relevansi yang erat dengan perlindungan terhadap sistem elektronik pemerintah. Serangan terhadap sistem pemerintah dapat menimbulkan

berbagai dampak, mulai dari terganggunya penyediaan informasi hingga menurunnya kepercayaan masyarakat terhadap kemampuan institusi negara dalam menjaga sistem digitalnya. Oleh karena itu, fungsi BSSN dalam melakukan deteksi, proteksi, penanggulangan, dan pemulihan menjadi bagian penting dalam menjaga keberlangsungan sistem elektronik pemerintah. Fungsi tersebut juga menunjukkan bahwa keberhasilan keamanan siber tidak hanya diukur dari kemampuan mencegah serangan, tetapi juga dari kemampuan institusi dalam merespons dan memulihkan sistem ketika serangan berhasil terjadi. Hal ini menjadi relevan dalam penelitian mengenai web *defacement* situs Pusmanas karena serangan tersebut terjadi terhadap sistem yang berada dalam lingkungan BSSN, sehingga kemampuan BSSN dalam menjalankan fungsi keamanan sibernya menjadi aspek penting untuk dipahami sebelum melakukan analisis terhadap respons yang diberikan.

Lebih lanjut, BSSN memiliki fungsi dalam melakukan evaluasi terhadap penyelenggaraan keamanan siber dan persandian. Evaluasi diperlukan untuk mengetahui sejauh mana mekanisme keamanan yang telah diterapkan mampu menghadapi ancaman serta untuk mengidentifikasi kelemahan yang masih terdapat dalam sistem. Hasil evaluasi dapat digunakan sebagai dasar untuk melakukan perbaikan terhadap kebijakan, prosedur, maupun mekanisme perlindungan sistem elektronik. Dalam konteks insiden keamanan siber, evaluasi pasca-serangan menjadi penting karena suatu insiden tidak hanya perlu diselesaikan melalui pemulihan

sistem, tetapi juga perlu dijadikan sebagai bahan pembelajaran untuk mencegah terulangnya serangan serupa. Dengan demikian, fungsi evaluasi BSSN memiliki keterkaitan dengan upaya membangun ketahanan siber (*cyber resilience*) dan meningkatkan kemampuan institusi dalam menghadapi ancaman pada masa mendatang (Republik Indonesia, 2021).

Berdasarkan uraian tersebut, tugas dan fungsi BSSN menunjukkan bahwa lembaga ini memiliki tanggung jawab dalam seluruh rangkaian pengelolaan keamanan siber, mulai dari identifikasi dan deteksi ancaman, perlindungan sistem, penanggulangan ketika insiden terjadi, pemulihan sistem, hingga evaluasi setelah insiden. Rangkaian tersebut menjadi penting dalam konteks penelitian karena dapat digunakan untuk melihat bagaimana mandat kelembagaan BSSN seharusnya diterapkan ketika menghadapi serangan terhadap sistem yang berada di bawah pengelolaannya. Dalam kasus web *defacement* situs Pusmanas tahun 2021, fungsi-fungsi tersebut menjadi dasar untuk memahami tindakan BSSN sebelum, selama, dan setelah serangan terjadi. Dengan demikian, pembahasan mengenai tugas dan fungsi BSSN tidak hanya memberikan gambaran mengenai kewenangan kelembagaan, tetapi juga menjadi dasar untuk memahami respons BSSN yang selanjutnya akan dianalisis melalui tahapan *Pre-Crisis Stage*, *Acute Crisis Stage*, *Chronic Stage*, dan *Resolution Stage* dalam *Crisis Management Theory* pada Bab 3 (Republik Indonesia, 2021).

2.2. Gambaran Umum Kasus *Defacement*

Web *defacement* merupakan salah satu bentuk serangan siber yang menargetkan integritas suatu situs web dengan cara mengubah tampilan, konten, maupun informasi yang ditampilkan tanpa izin dari pemilik sistem. Serangan ini umumnya dilakukan setelah pelaku berhasil memperoleh akses tidak sah (unauthorized access) ke server atau aplikasi web melalui pemanfaatan berbagai celah keamanan, seperti kerentanan pada aplikasi (web application vulnerabilities), konfigurasi server yang tidak aman, kelemahan autentikasi, maupun perangkat lunak yang tidak diperbarui secara berkala (National Institute of Standards and Technology [NIST], 2018). Berbeda dengan serangan yang bertujuan mencuri data atau memperoleh keuntungan finansial, web *defacement* lebih sering dimanfaatkan sebagai sarana untuk menunjukkan keberhasilan pelaku dalam menembus sistem keamanan, menyampaikan pesan politik maupun ideologis, melakukan protes terhadap suatu institusi, atau sekadar memperoleh pengakuan dari komunitas peretas.

Dalam perkembangannya, web *defacement* tidak lagi dipandang sebagai gangguan teknis yang hanya memengaruhi tampilan sebuah situs web. Serangan ini juga mencerminkan adanya kelemahan pada sistem keamanan informasi yang dimiliki oleh suatu organisasi. Keberhasilan pelaku mengubah tampilan situs menunjukkan bahwa mekanisme pengamanan yang diterapkan belum mampu mencegah akses tidak sah terhadap sistem. Oleh karena itu, insiden *defacement* sering dijadikan indikator awal untuk menilai tingkat kematangan (maturity) keamanan siber suatu organisasi, terutama dalam aspek pengelolaan kerentanan,

pengamanan aplikasi web, serta implementasi kebijakan keamanan informasi (Center for Internet Security [CIS], 2021).

Dalam konteks penyelenggaraan pemerintahan, web *defacement* memiliki dampak yang lebih luas dibandingkan terhadap organisasi swasta. Situs web pemerintah merupakan salah satu media utama dalam penyampaian informasi publik, pelayanan administrasi, maupun komunikasi antara pemerintah dengan masyarakat. Ketika sebuah situs pemerintah mengalami *defacement*, dampak yang ditimbulkan tidak hanya berupa terganggunya layanan informasi, tetapi juga dapat menurunkan tingkat kepercayaan masyarakat terhadap kemampuan pemerintah dalam menjaga keamanan sistem digital yang dikelolanya. Selain itu, insiden tersebut juga berpotensi memengaruhi kredibilitas institusi, terutama apabila yang menjadi sasaran merupakan lembaga yang memiliki tanggung jawab di bidang keamanan informasi atau keamanan siber nasional (Badan Siber dan Sandi Negara [BSSN], 2022).

Di Indonesia, insiden web *defacement* masih menjadi salah satu bentuk serangan siber yang cukup sering ditemukan pada berbagai situs pemerintah maupun sektor publik lainnya. Meskipun sebagian besar serangan *defacement* tidak selalu menyebabkan kebocoran data, keberhasilan pelaku dalam memperoleh akses terhadap sistem tetap menunjukkan adanya kelemahan pada mekanisme pengamanan yang diterapkan. Kondisi tersebut menjadi perhatian penting mengingat transformasi digital pemerintahan yang semakin berkembang turut meningkatkan ketergantungan terhadap keamanan infrastruktur teknologi informasi. Oleh karena itu, setiap insiden web *defacement* perlu dipandang sebagai

bagian dari tantangan keamanan siber nasional yang memerlukan respons tidak hanya dari aspek teknis, tetapi juga melalui penguatan tata kelola, kebijakan, dan koordinasi antarinstansi.

Berdasarkan kondisi tersebut, penelitian ini memfokuskan pembahasan pada insiden web *defacement* yang terjadi pada situs Pusat Malware Nasional (Pusmanas) milik Badan Siber dan Sandi Negara (BSSN) pada tahun 2021. Kasus ini dipilih karena memiliki karakteristik yang berbeda dibandingkan insiden *defacement* pada umumnya. Sebagai lembaga yang memiliki mandat dalam menjaga keamanan siber nasional, BSSN diharapkan mampu menerapkan mekanisme pencegahan, deteksi, dan penanganan insiden yang memadai terhadap sistem elektronik yang berada di bawah pengelolaannya. Oleh karena itu, insiden tersebut menjadi relevan untuk dianalisis lebih lanjut guna memahami bagaimana respons yang dilakukan BSSN dalam menghadapi krisis keamanan siber berdasarkan tahapan dalam Crisis Management Theory.

2.3. Kronologi Terjadinya Serangan *Defacement*

Pusat Malware Nasional (Pusmanas) merupakan salah satu unit yang berada dibawah Badan Siber dan Sandi Negara (BSSN) yang memiliki fungsi strategis dalam mendukung sistem keamanan siber nasional Indonesia. Pusmanas berperan dalam melakukan pemantauan, analisis, dan penyediaan informasi terkait ancaman malware serta aktivitas siber berbahaya yang dapat mengganggu sistem elektronik nasional. Selain itu, Pusmanas juga menjadi media edukasi publik mengenai perkembangan ancaman siber dan pentingnya perlindungan sistem digital di era transformasi teknologi yang semakin berkembang. Sebagai bagian dari lembaga

negara yang bertanggung jawab terhadap keamanan siber nasional, keberadaan Pusmanas tidak hanya memiliki fungsi teknis, tetapi juga mencerminkan kesiapan pemerintah dalam menjaga stabilitas dan keamanan ruang digital nasional. Oleh karena itu, setiap gangguan terhadap sistem yang berada di bawah koordinasi BSSN dapat memberikan dampak yang lebih luas, baik secara teknis maupun reputasional.

Pada tahun 2021, situs resmi Pusat Malware Nasional (Pusmanas) mengalami serangan siber berupa web *defacement* yang menyebabkan perubahan tampilan halaman *website* secara tidak sah oleh pihak peretas. Dalam insiden tersebut, halaman utama *website* tidak lagi menampilkan informasi resmi milik institusi, melainkan diganti dengan tampilan dan pesan tertentu yang dibuat oleh pelaku peretasan. Kejadian ini kemudian menjadi perhatian publik karena serangan justru terjadi pada institusi yang memiliki tanggung jawab dalam menjaga keamanan siber nasional. Langkah penonaktifan sementara *website* merupakan tindakan yang umum dilakukan dalam penanganan insiden keamanan siber. Tujuan utama tindakan tersebut adalah mencegah eksploitasi lanjutan terhadap sistem yang telah berhasil ditembus, sekaligus memberikan ruang bagi tim respons insiden untuk melakukan proses identifikasi kerentanan tanpa adanya gangguan dari aktivitas eksternal. Dalam praktik manajemen keamanan informasi, isolasi sistem menjadi salah satu prosedur awal yang dilakukan sebelum proses investigasi digital forensik dilaksanakan agar integritas bukti digital tetap terjaga.

Berdasarkan informasi yang beredar melalui berbagai media massa dan platform digital, *website* Pusmanas sempat tidak bisa diakses secara normal selama proses penanganan dilakukan. Sebagai langkah awal penanganan, sistem yang

terdampak kemudian dinonaktifkan sementara untuk mencegah potensi kerusakan yang lebih luas serta menghindari kemungkinan adanya akses ilegal lanjutan terhadap server dan sistem internal. Penonaktifan sementara tersebut dilakukan sebagai bagian dari prosedur pengamanan sistem dan proses investigasi awal terhadap sumber serangan. Dalam konteks keamanan siber, langkah isolasi sistem merupakan tindakan umum yang dilakukan ketika suatu sistem mengalami kompromi keamanan, terutama untuk membatasi penyebaran dampak dan menjaga integritas data yang masih tersimpan di dalam sistem.

Secara umum, serangan *defacement* dapat terjadi akibat adanya kerentanan pada sistem *website*, seperti kelemahan konfigurasi server, penggunaan perangkat lunak yang belum diperbarui, lemahnya sistem autentikasi, atau adanya celah keamanan pada aplikasi web yang digunakan. Dalam konteks kasus Pusmanas, terjadinya serangan tersebut menunjukkan bahwa masih terdapat potensi kerentanan pada sistem keamanan digital pemerintah yang dapat dimanfaatkan oleh pelaku serangan siber. Hal ini menunjukkan bahwa ancaman terhadap sistem elektronik pemerintah tidak hanya berasal dari kompleksitas teknologi, tetapi juga berkaitan dengan kesiapan tata kelola keamanan, kualitas pengawasan sistem, serta implementasi standar keamanan yang belum sepenuhnya optimal di tingkat institusi.

Selain berdampak terhadap operasional *website*, insiden ini juga memunculkan berbagai reaksi publik yang mempertanyakan efektivitas sistem keamanan siber nasional Indonesia. Banyak pihak menilai bahwa peretasan terhadap situs yang berada di bawah koordinasi BSSN menjadi simbol lemahnya

perlindungan infrastruktur digital pemerintah. Dalam konteks keamanan nasional, serangan terhadap *website* pemerintah tidak hanya dipandang sebagai gangguan teknis semata, tetapi juga sebagai ancaman terhadap kredibilitas institusi negara di ruang digital. *Website* pemerintah memiliki fungsi penting sebagai media pelayanan informasi publik, sehingga ketika sistem tersebut berhasil diretas, maka tingkat kepercayaan masyarakat terhadap kemampuan negara dalam menjaga keamanan data dan sistem elektronik dapat mengalami penurunan.

Karakteristik serangan *defacement* pada situs pemerintah juga memiliki dimensi simbolik dan psikologis. Dalam banyak kasus, tujuan utama pelaku tidak selalu untuk mencuri data, tetapi untuk menunjukkan bahwa sistem keamanan suatu institusi berhasil ditembus. Oleh karena itu, serangan semacam ini sering digunakan sebagai bentuk demonstrasi kemampuan pelaku sekaligus pesan simbolik mengenai lemahnya perlindungan sistem digital yang dimiliki suatu institusi. Dalam kasus Pusmanas, serangan tersebut memperlihatkan bahwa bahkan lembaga yang memiliki fungsi strategis dalam keamanan siber tetap memiliki risiko terhadap ancaman digital apabila pengawasan keamanan dan implementasi perlindungan sistem belum dilakukan secara maksimal.

Insiden *defacement* yang terjadi pada situs Pusmanas juga menunjukkan bahwa ancaman siber saat ini tidak selalu bertujuan untuk mencuri data atau memperoleh keuntungan finansial. Dalam banyak kasus, web *defacement* lebih sering digunakan sebagai bentuk demonstrasi kemampuan (*proof of capability*), penyampaian pesan politik (*hacktivism*), maupun upaya menunjukkan keberhasilan pelaku dalam menembus sistem keamanan suatu institusi. Meskipun BSSN

menyatakan bahwa tidak terjadi kebocoran data pada insiden ini, keberhasilan pelaku mengubah tampilan *website* tetap menunjukkan adanya celah keamanan yang berhasil dieksploitasi. Oleh karena itu, insiden ini tetap memiliki nilai strategis untuk dianalisis karena memperlihatkan bahwa perlindungan terhadap sistem elektronik pemerintah masih menghadapi tantangan dalam aspek pencegahan dan pengamanan infrastruktur digital.

Insiden *defacement* terhadap situs Pusmanas juga memberikan dampak terhadap tata kelola keamanan siber nasional secara lebih luas. Kasus ini menunjukkan bahwa masih terdapat tantangan dalam implementasi kebijakan keamanan siber di Indonesia, khususnya terkait kesiapan infrastruktur digital pemerintah, koordinasi antar lembaga, serta konsistensi penerapan standar keamanan sistem informasi. Selain itu, minimnya informasi publik terkait hasil investigasi dan langkah pemulihan pasca insiden juga menimbulkan pertanyaan mengenai transparansi dalam proses penanganan krisis siber pemerintah. Dalam manajemen keamanan siber modern, transparansi prosedural menjadi salah satu aspek penting untuk menjaga akuntabilitas institusi sekaligus meningkatkan kepercayaan publik terhadap kemampuan negara dalam menangani ancaman digital.