

BAB IV

KESIMPULAN DAN SARAN

4.1. Kesimpulan

Berdasarkan analisis menggunakan *Crisis Management Theory*, dapat disimpulkan bahwa efektivitas respons BSSN dipengaruhi oleh kualitas implementasi kebijakan pada aspek kejelasan tujuan kebijakan, ketersediaan sumber daya, koordinasi antarorganisasi, serta pengawasan dan kepatuhan terhadap standar keamanan siber.

Pada tahap pre-crisis, BSSN telah memiliki dasar kelembagaan dan regulasi yang mengatur pengamanan sistem elektronik serta penanganan insiden siber. Namun, terjadinya *web defacement* terhadap situs Pusmanas menunjukkan bahwa implementasi kebijakan pencegahan belum mampu menghilangkan seluruh kerentanan pada sistem yang berada dalam lingkungan BSSN. Kondisi ini menunjukkan bahwa keberadaan regulasi dan standar keamanan belum sepenuhnya diikuti dengan penerapan pengamanan yang konsisten pada tingkat institusi.

Pada tahap *acute crisis* dan *chronic stage*, respons BSSN menunjukkan hasil yang relatif lebih baik. BSSN mampu melakukan tindakan pengendalian terhadap sistem yang terdampak melalui penonaktifan sementara *website*, proses investigasi, serta pemulihan layanan digital. Hal tersebut menunjukkan bahwa kapasitas respons terhadap insiden telah berjalan, meskipun efektivitasnya masih dipengaruhi oleh keterbatasan koordinasi, komunikasi publik, dan transparansi hasil investigasi.

Sementara itu, pada tahap *resolution*, penelitian menemukan bahwa sistem berhasil dipulihkan, tetapi pembelajaran kelembagaan dan evaluasi pasca-insiden

belum terlihat secara optimal. Belum terdapat bukti yang kuat mengenai perubahan prosedur atau mekanisme keamanan yang secara langsung dihasilkan dari kasus Pusmanas. Dengan demikian, penelitian ini menyimpulkan bahwa respons BSSN terhadap serangan *web defacement* Pusmanas tahun 2021 belum sepenuhnya efektif atau bersifat parsial, karena efektivitas lebih terlihat pada aspek respons dan pemulihan dibandingkan pada aspek pencegahan serta evaluasi pasca-krisis.

Secara keseluruhan, penelitian ini menemukan adanya implementation gap antara kerangka regulasi keamanan siber dengan implementasinya pada kasus web defacement situs Pusmanas tahun 2021. Pada aspek pengamanan sistem, kesenjangan terlihat dari masih terjadinya kompromi terhadap sistem meskipun telah tersedia kerangka pengamanan melalui Peraturan BSSN Nomor 8 Tahun 2020. Pada aspek penanganan insiden, BSSN telah melakukan respons awal melalui pengamanan dan pemulihan sistem, tetapi dokumentasi mengenai penerapan mekanisme Tim Tanggap Insiden Siber sebagaimana diatur dalam Peraturan BSSN Nomor 10 Tahun 2020 masih terbatas. Sementara itu, pada aspek evaluasi dan perbaikan berkelanjutan, pemulihan website telah dilakukan, tetapi bukti mengenai evaluasi pasca-insiden dan pembelajaran kelembagaan berdasarkan Peraturan BSSN Nomor 4 Tahun 2021 belum terlihat secara kuat.

Dengan demikian, implementation gap pada kasus Pusmanas terutama terlihat pada ketidaksesuaian antara standar normatif, pelaksanaan pencegahan dan respons, serta tindak lanjut evaluasi setelah insiden.

4.2. Saran

Berdasarkan hasil penelitian, terdapat beberapa rekomendasi yang dapat dipertimbangkan untuk meningkatkan efektivitas implementasi kebijakan keamanan siber di Indonesia.

4.2.1. Bagi Badan Siber dan Sandi Negara (BSSN)

BSSN perlu memperkuat mekanisme pencegahan melalui peningkatan monitoring kerentanan, audit keamanan secara berkala, serta penerapan standar keamanan yang lebih konsisten pada seluruh sistem elektronik pemerintah. Selain itu, BSSN juga perlu meningkatkan transparansi dalam penyampaian informasi mengenai penanganan insiden agar proses evaluasi dan pembelajaran kelembagaan dapat berjalan lebih efektif.

4.2.2. Bagi Pemerintah Indonesia

Pemerintah perlu memperkuat implementasi kebijakan keamanan siber melalui peningkatan koordinasi antar kementerian, lembaga, dan pemerintah daerah dalam penyelenggaraan keamanan sistem elektronik. Penguatan kapasitas sumber daya manusia, penyediaan anggaran yang memadai, serta harmonisasi regulasi juga menjadi langkah penting untuk mengurangi kesenjangan implementasi kebijakan pada berbagai institusi pemerintah.

4.2.3. Bagi Penelitian Selanjutnya

Penelitian ini masih berfokus pada satu studi kasus, yaitu serangan web *defacement* terhadap situs Pusmanas tahun 2021. Oleh karena itu,

penelitian selanjutnya disarankan melakukan analisis komparatif terhadap beberapa insiden siber pada institusi pemerintah lainnya atau membandingkan implementasi kebijakan keamanan siber Indonesia dengan negara lain. Pendekatan tersebut diharapkan dapat memberikan gambaran yang lebih komprehensif mengenai efektivitas tata kelola keamanan siber nasional.