BAB VI
SIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan dari temuan-temuan yang penulis temukan maka dapat didapatkan beberapa strategi yang digunakan oleh Europol dalam merespons serangan ransomware wannacry. Strategi yang pertama adalah melakukan koordinasi internasional dan kemitraan strategis, strategi yang pertama ini awalnya dilakukan oleh Uni Eropa dengan merespons cepat dan terkoordinasi terhadap serangan WannaCry pada Mei 2017. Komisi Eropa dan ENISA segera mengeluarkan peringatan serta panduan mitigasi, mendesak penerapan *patch* keamanan dari Microsoft. Insiden ini juga mempercepat penerapan NIS Directive, yang mewajibkan negara anggota meningkatkan kapasitas keamanan siber dan berbagi informasi ancaman. Europol melalui *European Cybercrime Centre* (EC3), menjalin kemitraan strategis dengan lembaga internasional seperti INTERPOL, FBI, *National Crime Agency* (NCA) Inggris, serta unit penegakan hukum nasional dari negara-negara anggota Uni Eropa dan negara mitra lainnya. Kemitraan ini mendukung pertukaran intelijen siber *real-time*, mempercepat forensik digital, dan memungkinkan analisis menyeluruh terhadap asal, pola, serta penyebaran *malware* WannaCry. Europol juga turut mengaktifkan *Joint Cybercrime Action Taskforce* (J-CAT) untuk mengoordinasikan operasi internasional melawan pelaku kejahatan siber, memfasilitasi pemetaan infrastruktur serangan, identifikasi *botnet*, dan pelacakan dana tebusan berbasis kripto. Selain itu Europol juga menjalin Kerja sama dengan sektor swasta, seperti Microsoft yang merilis patch keamanan dan membantu investigasi teknis, juga menjadi elemen krusial dalam mitigasi serangan.

Strategi kedua yang diambil oleh Europol adalah analisis ancaman dan intelijen siber, dalam hal ini Europol berperan sebagai pusat koordinasi utama dalam penanganan kejahatan siber, memimpin upaya koordinasi respons antarnegara dan memperlancar pertukaran informasi sensitif dan vital. Ini termasuk menyuplai data ancaman, analisis teknis, serta koordinasi respons cepat lintas

negara melalui EC3. Selain itu Jaringan CSIRT yang diatur dalam NIS Directive diaktifkan untuk mempercepat pertukaran informasi terkait serangan, seperti indikator kompromi dan *patch* keamanan. ENISA juga berperan sebagai koordinator, mengumpulkan data, menganalisis tren, dan menyebarkan laporan ancaman terintegrasi di tingkat Uni Eropa. Dan strategi ketiga yang diambil Europol adalah peningkatan kesadaran publik dan pencegahan, Europol melalui EC3 mengeluarkan peringatan publik mengenai skala ancaman dan risiko yang berkembang dari WannaCry, serta memberikan informasi rinci tentang cara kerja virus dan langkah-langkah pencegahan yang harus diambil. Mereka secara aktif mendesak organisasi dan individu untuk segera menerapkan patch keamanan dari Microsoft yang dapat menambal celah "EternalBlue". Strategi ini berorientasi pada pemberdayaan masyarakat sipil sebagai benteng pertama dalam menghadapi *ransomware* dengan menyediakan alat bantu teknis (seperti *decryptor*) dan informasi praktis mengenai praktik keamanan siber dasar melalui inisiatif seperti "No More Ransom".

Penurunan kasus WannaCry pasca implementasi strategi Europol dan mitranya menunjukkan keberhasilan signifikan dari pendekatan terkoordinasi tersebut. Setelah serangan masif pada Mei 2017, Uni Eropa dan lembaga-lembaga seperti Europol (melalui EC3) merespons dengan cepat dan terpadu. Implementasi NIS Directive, yang mewajibkan negara anggota meningkatkan kapasitas keamanan siber dan berbagi informasi, memperkuat pertahanan kolektif. Koordinasi internasional yang intensif, termasuk pertukaran intelijen *real-time* dan operasi penegakan hukum lintas batas, memungkinkan identifikasi dan penindakan terhadap infrastruktur serangan serta pelacakan pelaku. Selain itu, kampanye peningkatan kesadaran publik dan penyediaan alat bantu seperti "No More Ransom" secara efektif memberdayakan individu dan organisasi untuk melindungi diri. Hasil dari upaya komprehensif ini adalah penurunan tajam insiden WannaCry di Eropa antara tahun 2017 dan 2018, dengan tidak adanya lonjakan signifikan dari varian WannaCry sejak pertengahan 2018 di Uni Eropa. Ini menunjukkan bahwa strategi proaktif dan kolaboratif Europol berhasil dalam membangun ketahanan siber yang kuat, secara efektif menekan penyebaran dan dampak dari *ransomware* tersebut.

Dari semua penjelasan yang telah penulis tuliskan, dapat disimpulkan bahwa dalam menghadapi kejahatan siber seperti ransomware WannaCry, kerja sama internasional menjadi kunci utama untuk penanganan dan pemberatasan serangan siber. Karena kejahatan siber adalah kejahatan lintas negara yang tidak bisa diselesaikan oleh satu negara saja. Europol membuktikan bahwa kerja sama antar negara, saling berbagi informasi, berbagi keahlian, serta adanya sistem koordinasi yang kuat sangat efektif dalam mengurangi dampak serangan. Selain itu, serangan ransomware wannacry juga dapat memberikan pelajaran penting bagi semua pihak bahwa keamanan siber bukan hanya tugas pemerintah maupun lembaga penegak hukum saja, tetapi juga menjadi tanggung jawab bersama antara pemerintah, sektor swasta, perusahaan teknologi, serta masyarakat pengguna teknologi itu sendiri.

6.2 Saran

Berdasarkan penelitian dan Kesimpulan yang penulis tulis terdapat beberapa saran atau masukan dari penulis yang bertujuan untuk peningkatan dalam penanganan siber yang mungkin akan terjadi di masa yang akan datang. Saran ini diharapkan dapat berguna bagi para pihak terkait baik Europol, negara anggota Uni Eropa, maupun pihak-pihak yang menggunakan teknologi informasi dalam hidupnya. Saran untuk Europol adalah memperkuat jaringan kerja internasional, regional maupun swatsa yang telah ada. Selain itu saran untuk Europol adalah memperluas jaringan kerjasamanya maupun kolaborasinya yang sangat berguna untuk memperluas jangkauan kerjasama, proses pertukaran informasi, penelusuran pelaku, serta pengembangan teknologi pencegahan dapat dilakukan secara lebih cepat dan efektif dalam menghadapi serangan siber yang bersifat lintas batas. Lalu saran untuk Europol, Organisasi Internasional maupun negara-negara adalah melakukan penguatan sistem keamanan siber menjadi salah satu skala prioritas karema kejahatan siber tidak hanya merugikan satu individu teteapi juga turut merugikan negara bahkan merugikan secara global. Dengan adanya hal itu negara-negara disarankan mengembangkan suatu sistem yang berguna untuk mendeteksi serangan secara dini. Saran lainnya adalah para pemirintah dari suatu negara erlu membangun lembaga koordinasi keamanan siber nasional, mengatur kebijakan

keamanan digital, memperkuat kemampuan sumber daya manusia di bidang siber, serta menjalin kerja sama dengan organisasi internasional agar lebih siap menghadapi serangan siber di masa depan.

Lalu saran berikutnya untuk seluruh individu di dunia untuk meningkatkan edukasi dan kesadaran diri akan bahaya kejahatan siber. Masing-masing individu harus lebih peduli terhadap ancaman siber dengan cara memperbarui sistem komputer secara berkala maupun melakukan pencadangan data secara rutin agar data kalian tidak hilang secara keseluruhan. Selain itu saran untuk individu adalah lebih berhati-hati dalam penggunaan internet, karena virus tersebut bisa memasuki perangkat kalian dengan tautan link maupun webstie tidak resmi yang kalian buka. Lalu saran lainnya adalah tidak menggunakan perangkat lunak bajakan atau tidak resmi, karena perangkat tersebut berpotensi memiliki virus didalammnya yang bisa saja dapat mencuri data anda atau bahkan diperdagangkannya data pribadi anda. Selain itu individu harus membuat kata sandi yang kuat, tidak mudah ditebak, dan tidak berhubungan dengan hal pribadi yang mudah diketahui oleh orang lain karena jika kata sandi anda mudah untuk ditebak para pelaku kejahatan bisa mencari celah untuk mengambil data yang anda miliki. Dan saran terkahir adalah memasang anti virus pada perangkat anda, sehingga memudahkan anda dalam pendekteksian adanya virus pada perangkat anda.

Dengan berbagai saran yang telah disampaikan, diharapkan seluruh pihak yang berkepentingan, baik lembaga penegak hukum internasional seperti Europol, negara-negara anggota Uni Eropa, organisasi internasional, pemerintah masing-masing negara, maupun individu, dapat mengambil langkah-langkah konkret dalam menghadapi tantangan kejahatan siber yang semakin kompleks di masa depan. Kolaborasi yang kuat, penguatan sistem keamanan, peningkatan kapasitas sumber daya manusia, serta kesadaran individu dalam menjaga keamanan data pribadi merupakan kunci utama dalam menciptakan ekosistem digital yang aman dan terpercaya. Semoga saran-saran ini dapat menjadi kontribusi positif dan memberikan manfaat dalam upaya pencegahan serta penanggulangan kejahatan siber secara global.