ABSTRAK

Serangan ransomware WannaCry yang terjadi pada tahun 2017 menjadi salah satu serangan siber terbesar yang berdampak secara global. Ransomware ini menyebar sangat cepat dengan mengeksploitasi kelemahan sistem operasi Windows melalui celah EternalBlue, sehingga mengunci data korban dan menuntut pembayaran tebusan dalam bentuk Bitcoin. Ancaman yang bersifat lintas negara ini menuntut adanya penanganan secara kolektif dan terkoordinasi di tingkat internasional. Europol sebagai lembaga penegak hukum Uni Eropa memiliki peran penting dalam merespons serangan ini. Penelitian ini bertujuan untuk menganalisis strategi yang diterapkan oleh Europol dalam menangani serangan ransomware WannaCry, khususnya dalam aspek koordinasi internasional. Metode penelitian menggunakan pendekatan kualitatif deskriptif dengan teknik studi dokumentasi dari berbagai sumber resmi, jurnal akademik, laporan lembaga internasional, serta berita terkait. Hasil penelitian menunjukkan bahwa strategi Europol menitikberatkan pada penguatan kerja sama internasional melalui koordinasi antar negara anggota Uni Eropa, lembaga internasional seperti Interpol dan FBI, serta sektor swasta, termasuk perusahaan keamanan siber. Melalui European Cybercrime Centre (EC3) dan Joint Cybercrime Action Taskforce (J-CAT), Europol mengoordinasikan pertukaran data intelijen, forensik digital, serta pemberian peringatan dini kepada seluruh negara anggota.

Kata Kunci: Europol, Ransomware WannaCry, Keamanan Siber, Kejahatan Siber, Strategi Penanganan, Kerja Sama Internasional.

ABSTRACT

The WannaCry ransomware attack that occurred in 2017 was one of the largest cyber attacks that had a global impact. This ransomware spread very quickly by exploiting the weaknesses of the Windows operating system through the EternalBlue vulnerability, thus locking the victim's data and demanding ransom payments in Bitcoin. This cross-border threat demands collective and coordinated handling at the international level. Europol as the European Union's law enforcement agency has an important role in responding to this attack. This study aims to analyze the strategies implemented by Europol in handling the WannaCry ransomware attack, especially in terms of international coordination. The research method uses a descriptive qualitative approach with documentation study techniques from various official sources, academic journals, international agency reports, and related news. The results of the study show that Europol's strategy focuses on strengthening international cooperation through coordination between EU member states, international institutions such as Interpol and the FBI, and the private sector, including cybersecurity companies. Through the European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT), Europol coordinates the exchange of intelligence data, digital forensics, and the provision of early warnings to all member states.

Keywords: Europol, WannaCry Ransomware, Cybersecurity, Cybercrime, Response Strategy, International Cooperation.