UPAYA KEPOLISIAN DALAM RANGKA MENJAGA KEAMANAN SISTEM M-BANKING TERHADAP ANCAMAN SERANGAN SIBER MELALUI TEKNIK *SCAMMING*

ABSTRAK

Oleh

DICKY PUTRA ARUMAWAN

Aktivitas *online* saat ini telah menjadi bagian besar dari kegiatan masyarakat dunia. Bersamaan dengan meningkatnya penggunaan *m-banking*, muncul pula berbagai ancaman keamanan siber yang mengintai. Salah satu ancaman tersebut adalah serangan *scamming*, tujuan dalam penulisan tesis ini adalah untuk menganalisis dan memahami upaya kepolisian dalam rangka menjaga keamanan sistem *m-banking* terhadap ancaman serangan siber melalui teknik *scamming* dan untuk menganalisis dan memahami kendala kepolisian dalam rangka menjaga keamanan sistem *m-banking* terhadap ancaman serangan siber melalui teknik *scamming.*

Penelitian ini menggunakan pendekatan yuridis normatif dan empiris. penelitian normatif dilakukan terhadap hal-hal yang bersifat teoritis asas-asas hukum, sedangkan pendekatan empiris yaitu dilakukan untuk mempelajari hukum dalam kenyataannya baik berupa penilaian perilaku hukum yang didasarkan pada identifikasai hukum dan efektifitas hukum.

Adapun hasil penelitian yang didapatkan bahwa dalam rangka menjaga keamanan sistem *M-Banking* terhadap serangan *scamming*, upaya kepolisian sangat penting. dalam analisis ini, kita melihat bahwa kepolisian telah menerapkan langkah-langkah preventif dan represif yang efektif, sejalan dengan teori penanggulangan kejahatan. Langkah-langkah preventif, seperti kampanye kesadaran dan edukasi keamanan digital, dan langkah-langkah represif, seperti deteksi dini, investigasi mendalam, penangkapan pelaku, dan penuntutan hukum yang efektif, memberikan sanksi yang tegas kepada para pelaku serangan *scamming*. Ini memberikan efek jera kepada pelaku dan memberikan keadilan kepada korban. Kendala kepolisian dalam rangka menjaga keamanan sistem *m-banking* terhadap ancaman serangan siber melalui teknik *scamming* meliputi: keterbatasan personil seperti tenaga ahli IT dan *cyber forensic*. Kendala lain yang krusial adalah terbatasnya dana anggaran operasional, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cyber crime* dan lemahnya pengawasan penggunaan internet berpotensi besar akan menciptakan peluang terjadinya kejahatan *cyber crime* (dunia maya).

Adapun saran yang dapat disampaikan dalam penelitian ini sebagai berikut: Sebaiknya para praktisi juga bisa berperan penting dalam memberikan masukan-masukan kepada pihak pemerintah dalam keamanan jaringan komputer dan internet dan sebaiknya kepolisian perlu mengembangkan kapasitas mereka dalam menghadapi serangan siber. Ini melibatkan pelatihan dan pengembangan keterampilan yang diperlukan dalam bidang keamanan siber

Kata Kunci: Upaya Kepolisian, *M-Banking, Cyber Scamming*

POLICE EFFORTS IN ORDER TO KEEP M-BANKING SECURITY SYSTEM FROM CYBER ATTACK THREAT THROUGH SCAMMING TECHNIQUE

ABSTRACT

By Dicky Putra Arumawan

Online activity recently has become big part of world society events. Along with increasing of m-banking usage, also appears some threats of cyber security attacks which lurks. One of the threat is scamming attack, the purposes of this thesis writing are to analyze and to understand police efforts in order to keep m-banking security system from cyber attack threat through scamming technique and to analyze and to understand police constraints in order to keep m-banking security system from cyber attack threat through scamming technique.

This research is use normative juridical and empirical approach. Normative research is carried out on theoretical matters of legal principles, While the empirical approach is carried out to study the law in reality both in the form of an assessment of legal behavior based on legal identity and legal effectiveness.

The results of the research obtained that in order to maintain the security of the M-Banking system against scamming attacks, police efforts are important. In this analysis, we see that the police force has implemented effective preventive and repressive measures, in line with the theory of legal countermeasures. Preventive measures, such as digital safety awareness and education campaigns, and repressive measures, such as early detection, in-depth investigations, arrests of perpetrators, and effective prosecution, provide strict sanctions to perpetrators of scamming attacks. It provides a deterrent effect to the perpetrator and provides justice to the victim and police constraints in order to maintain the security of the m-banking system against the threat of cyber attacks through scamming techniques include: limitations of personnel such as IT experts and cyber forensics. Another crucial obstacle is the limited operational budget funds, problems that are quite crucial in addition to legal tools, namely insufficient human resources, budget and facilities and infrastructure to support the disclosure of cyber crime cases and weak supervision of internet use has great potential to create opportunities for cyber crime.

The suggestions that can be conveyed in this study are as follows: Practitioners should also act an important role in providing input to the government on computer network and internet security and should police need to develop their capacity to deal with cyber attacks. This involves training and developing the necessary skills in the field of cyber security.

Keywords: Police Efforts, M-Banking, Cyber Scamming