

ABSTRAK

Skripsi dengan judul “Peran Bank Indonesia dalam Melawan Kejahatan Siber pada Layanan Mobile Banking Syariah” ditulis oleh Binzar Wimpi Nugraha, NIM 126401202059. Jurusan Ekonomi. Program Studi Perbankan Syariah, Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung, Dosen Pembimbing Dr. Binti Nur Asiyah, M.Si.

Penelitian ini dilatarbelakangi dengan adanya permasalahan baru yang terjadi pada dunia perbankan khususnya di perbankan syariah. Permasalahan baru tersebut yaitu adanya dugaan serangan siber pada layanan mobile banking syariah. Dengan adanya dugaan tersebut sudah terdapat efek yang terjadi yaitu Masyarakat atau nasabah tidak bisa mengakses mobile banking mereka, sehingga kegiatan perekonomian terganggu dan bisa dikatakan lumpuh sementara. Dengan adanya permasalahan itu, Bank Indonesia sebagai pembuat regulasi aspek pembayaran mempunyai peran yang sangat vital atas serangan kejahatan siber ini. Kebijakan- kebijakan yang diambil BI untuk melawan kejahatan siber ini diantaranya pembuatan platform untuk membagikan informasi berkonteks ancaman siber antara Lembaga bank yang ada di Indonesia dan BI, adanya cybersecurity yang dilakukan BI dan aturan-aturan BI tentang teknologi informasi. Rumusan masalah pada penelitian ini yaitu bagaimana kejahatan siber yang terjadi pada layanan mobile banking syariah? dan bagaimana peran bank Indonesia dalam melawan kejahatan siber pada layanan mobile banking syariah?

Penelitian ini menggunakan pendekatan kualitatif. Jenis studi kepustakaan menggunakan sumber dari PBI, POJK, buku, jurnal, *research* BI, website, artikel. Sumber data diperoleh dari sumber data sekunder. Selain itu teknik mengumpulkan data dengan menggunakan teknik pengumpulan data dari kajian literature, sedangkan Teknik analisis data dengan kondensasi data, penyajian data, verifikasi dan kesimpulan

Hasil penelitian yang diperoleh yaitu 1) Kejahatan siber yang terjadi pada layanan mobile banking khususnya syariah diantaranya yaitu *phising*, penyadapan data (*sniffing*), *keylogger*, identitas palsu (*spoofing*), mengalihkan situs (*pharming*), *ransomware*. Dengan kejahatan tersebut, nasabah sangat dirugikan. Contohnya adalah kehilangan uang. 2) peran Bank Indonesia dalam melawan kejahatan siber di layanan *Mobile Banking* Syariah yaitu dengan membuat kebijakan agar bank memperkuat kekuatan siber pada cakupan internal dan cakupan industry keuangan serta membangun dan memperkuat pusat ketahanan siber antar Lembaga di seluruh Indonesia. Rancangan ketahanan siber pada cakupan *human*, *process*, dan teknologinya, *cybersecurity* (sharing platform), *holistic*, regulasi kejahatan siber. Implikasi praktis penelitian ini agar peran BI dalam upaya melawan kejahatan siber lebih implementatif dan terukur. Maraknya kejahatan siber yang terjadi, Bank Indonesia bekerjasama dengan instansi terkait agar terciptanya peraturan penanganan kejahatan siber yang komprehensif.

Kata Kunci: Bank Indonesia, Kejahatan Siber, Mobile Banking Syariah

ABSTRACT

The thesis with the title "The Role of Bank Indonesia in Combating Cyber Crime on Sharia Mobile Banking Services" was written by Binzar Wimpi Nugraha, NIM 126401202059. Department of Economics. Sharia Banking Study Program, Faculty of Islamic Economics and Business, Sayyid Ali Rahmatullah State Islamic University Tulungagung, Supervisor Dr. Binti Nur Asiyah, M.Si.

This research is motivated by the existence of new problems that occur in the banking world, especially in sharia banking. The new problem is an alleged cyberattack on sharia mobile banking services. With this allegation, there are already effects that have occurred, namely that the public or customers cannot access their mobile banking, so that economic activities are disrupted and can be said to be temporarily paralyzed. Given these problems, Bank Indonesia as the regulator of payment aspects has a very vital role in dealing with this cybercrime attack. The policies taken by BI to fight cybercrime include the creation of a platform to share information in the context of cyber threats between banking institutions in Indonesia and BI, the existence of cybersecurity carried out by BI and BI regulations regarding information technology. The formulation of the problem in this research is how cybercrime occurs in sharia mobile banking services and the role of Indonesian banks in fighting cybercrime in sharia mobile banking services. In this research, researchers used a descriptive qualitative approach using secondary data, obtaining data from journals, books and the internet

This research uses a qualitative approach. This type of literature study uses sources from PBI, POJK, books, journals, BI research, websites, articles. Data sources were obtained from secondary data sources. Apart from that, data collection techniques use data collection techniques from literature studies, while data analysis techniques use data condensation, data presentation, verification and conclusions

The research results obtained are 1) Cybercrimes that occur in mobile banking services, especially sharia, include phishing, data interception (sniffing), keyloggers, fake identities (spoofing), redirecting sites (pharming), ransomware. With this crime, customers are greatly harmed. An example is losing money. 2) Bank Indonesia's role in fighting cybercrime in Sharia Mobile Banking services is by creating policies for banks to tighten cyber powers in internal and financial industry coverage as well as building and strengthening cyber resilience centers between institutions throughout Indonesia. Cyber resilience design covering human, process and technology, cybersecurity (sharing platform), holistic, cybercrime regulations. The practical implications of this research are that BI's role in fighting cybercrime is more implementing and measurable. With the rise of cybercrimes, Bank Indonesia is collaborating with related agencies to create comprehensive regulations for handling cybercrimes.

Keywords: *Bank Indonesia, Cyber Crime, Sharia Mobile Banking*

