e-ISSN:2829-4580, p-ISSN: 2829-4599
DOI: https://doi.org/10.38035/jim.v2i1
Received: 17 Mei 2023, Revised: 13 Juni 2023, Publish: 14 Juni 2023

JIM
JURNAL ILMU MULTIDISIPLIN
E-ISSN:2829-4580, P-ISSN=2829-4599
https://greenpub.org/JIM
editor@greenpub.org
0811 7401 455

Dampak Denial of Service pada Perusahaan Perbankan di Indonesia

Muhammad Julda Alhafiz[1], Achmad Fauzi[2], Akbar Dwiansyah[3], Bonita Revana Indriani[4], Fairly Maulana Andhito Putra[5], Ryan Ridho Ridwani[6]
[1.] Universitas Bhayangkara Jakarta Raya, Indonesia, mzuldaalhafizh@gmail.com
[2.] Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3.] Universitas Bhayangkara Jakarta Raya, Indonesia, akbardwiansyah7@gmail.com
[4.] Universitas Bhayangkara Jakarta Raya, Indonesia, bonitarevanaindriyani@gmail.com
[5.] Universitas Bhayangkara Jakarta Raya, Indonesia, fairlyandhito0@gmail.com
[6.] Universitas Bhayangkara Jakarta Raya, Indonesia, ryanridhor9@gmail.com

Corresponding Author: Muhammad Julda Alhafiz

Abstract: *In Indonesia's banking context, DoS attacks can have a major impact on the availability of banking services and harm both customers and the company itself. Therefore, it is important to understand the impact of DoS on banking companies in Indonesia to take appropriate preventive and remedial actions. This article will discuss the impact of DoS attacks on banking companies in Indonesia and the efforts that can be made to overcome these attacks. The research method used is the qualitative literature review method. The results of this discussion lead to the conclusion that overall, Denial of Service attacks have a serious impact on banking companies in Indonesia and need to be taken seriously by banking companies, regulators, and customers.*

Keyword: *DoS, Banking, Cybercrime.*

Abstrak: Dalam konteks perbankan Indonesia, serangan DoS dapat berdampak besar pada ketersediaan layanan perbankan dan merugikan nasabah maupun perusahaan itu sendiri. Oleh karena itu, penting untuk memahami dampak DoS terhadap perusahaan perbankan di Indonesia untuk mengambil tindakan pencegahan dan perbaikan yang tepat. Artikel ini akan membahas dampak serangan DoS terhadap perusahaan perbankan di Indonesia dan upaya yang dapat dilakukan untuk mengatasi serangan tersebut. Metode penelitian yang digunakan adalah metode kajian literatur kualitatif. Hasil pembahasan ini mengarah pada kesimpulan bahwa secara keseluruhan, serangan Denial of Service berdampak serius terhadap perusahaan perbankan di Indonesia dan perlu ditanggapi secara serius oleh perusahaan perbankan, regulator, dan nasabah.

Kata Kunci: DoS, Perbankan, Cybercrime.

PENDAHULUAN

Bank merupakan salah satu penyedia jasa keuangan yang telah memberikan jasa seperti surat berharga dan pinjaman kepada masyarakat dan perusahaan. Ketika bank pertama kali didirikan pada tahun 1955, bank tidak lebih dari layanan penukaran uang, yang kemudian menjadi layanan simpanan dan kemudian menjadi layanan tabungan. Untuk meningkatkan layanannya, bank telah menggunakan teknologi di berbagai bidang, termasuk ATM. ATM digunakan untuk menggantikan layanan teller dalam bertransaksi seperti tarik tunai dan transaksi lainnya.

Untuk menjalin hubungan jangka panjang dengan nasabah, bank harus selalu berhubungan dengan nasabah dan membuat mereka aman dan terpercaya, karena nasabah dapat dengan mudah mendapatkan informasi yang mereka butuhkan dari bank. Sejauh situs web dapat meningkatkan interaksi sosial, seperti keterbukaan, daya tanggap, dan kualitas informasi, hal itu memengaruhi kemampuan situs web untuk memenuhi kebutuhan online pengguna.

Dalam beberapa tahun terakhir, banyak bank Indonesia telah menerapkan strategi digital mereka di mobile banking. Pada tahun 2018, sebuah survei oleh PwC menemukan bahwa sepertiga orang Indonesia melakukan bisnis online (ponsel dan internet) sepanjang tahun. Nasabah menikmati kemudahan phone banking atau internet banking, karena dapat mengakses layanan secara langsung hingga 24 jam dibandingkan dengan cabang. Namun, penggunaan teknologi finansial ini bukannya tanpa risiko. Jika terjadi gangguan atau layanan yang tiba-tiba (offline), layanan perbankan/lainnya milik nasabah akan terputus. Salah satu hal yang dapat merugikan perbankan online adalah DoS (denial of service).

DoS sering dipicu dengan mengirimkan sejumlah besar paket dalam jangka waktu yang lama atau dengan mengirimkan sejumlah besar paket pada waktu yang sama dan mencekik server. Ada banyak alat di Internet dengan skrip PHP dan Perl, jadi tidak sulit untuk mengimplementasikan serangan ini. Banyak PC zombie berpartisipasi dalam serangan ini dan melakukan serangan DoS. Individu atau kelompok yang tidak bermoral dapat menggunakan Internet untuk memblokir atau menghapus situs web, mengalihkan router, dan menolak akses ke orang lain.

Oleh karena itu, DoS merugikan banyak pihak. Bank Indonesia baru-baru ini mengalami kebocoran data. Berita kebocoran data di Indonesia tersebar di media sosial pada awal tahun 2022. Akun Twitter @darktracer_int mengunggah tangkapan layar dengan deskripsi file tersebut dan menyebutkan bahwa file tersebut berasal dari www.bi.to.id. Dalam penyelidikan lain, pelanggaran data tersebut tampaknya terjadi secara berkala, dengan kebocoran pertama diperkirakan terjadi antara tahun 2021 dan 2022. Selama dua tahun terakhir, jumlah pelanggaran data bank di Indonesia terus meningkat karena jumlah peretasan alat telah meningkat.

Pencurian data merupakan masalah besar di era digital saat ini. Jika data yang dicuri jatuh ke tangan yang salah, itu bisa menjadi bumerang dan merugikan banyak orang lain. Kejadian serupa terjadi di Bank Indonesia dan beberapa bank lain di Indonesia. Salah satu aksi para hacker Rusia adalah membobol sistem dan mendapatkan data dari bank Indonesia. Padahal, pembobolan data ini menjadi perhatian utama banyak bank dan bank lain, mengingat kiprah Bank Indonesia yang menjadikannya sebagai bank sentral dan pusat distribusi keuangan Indonesia.

Didasarkan dari latar belakang diatas, maka dari itu dibuatlah rumusan masalah seperti berikut ini:

1. Apa saja jenis-jenis kasus kejahatan siber yang marak terjadi pada perbankan?
2. Apa dampak dari serangan denial of service pada perbankan?

3. Bagaimana cara perusahaan bank dalam mengatasi sistem yang terkena denial of service?

METODE

Dalam penelitian ini, metode yang digunakan yaitu metode kualitatif literatur review. Teknik ini bertujuan untuk memamparkan beragam teori yang sesuai dengan permasalahan yang saat ini diteliti menjadi bahan rujukan dalam pembahasan hasil penelitian. Waktu riset berlangsung sekitar satu bulan mulai dari bulan Maret hingga April 2023.

Tabel 1: Penelitian Terdahulu

No	Author, Tahun	Hasil Riset	Persamaan dengan Riset ini	Perbedaan dengan Riset ini
1.	(Chandra et al., 2021)	Beberapa perusahaan fokus pada penelitian dan model keamanan (kerangka kerja).	Faktor dari jenis-jenis serangan pada denial of service	Tidak ada pengaruh faktor analisis keamanan pada jurnal terdahulu.
2.	(Faridi, 2018)	Terdapat beberapa Kejahatan dunia maya di sektor perbankan menyebabkan kejahatan perbankan.	Faktor usulan solusi untuk mengatasi masalah cybercrime di sektor perbankan.	
3.	(Pratama et al., n.d.)	Terdapat pengaruh serangan DDoS di sektor perbankan serta solusi untuk mengatasinya.	Faktor dari pengaruh dan cara mengatasi serangan DDoS.	
4.	(Kusuma et al., 2022)	Terdapat laporan yang mengatur perlindungan data dan kasus Bank Indonesia dengan pelanggaran data.	Faktor dari Bank Indonesia yang mengalami kebocoran data.	Tidak ada cara untuk mengatasi kasus kebocoran data pada jurnal terdahulu.
5.	(Siregar, 2013)	Terdapat cara kerja, teknik, dampak, dan cara mengatasi serangan denial of service.	Faktor dari dampak serangan denial of service.	
6.	(Ratulangi et al., 2021)	Terdapat berbagai jenis kejahatan dunia maya dan penegakan hukum pidana terhadap penjahat dan bank.	Faktor dimana pelaku dapat melakukan kejahatan siber dengan beberapa cara.	
7.	(Hidayatullah, 2023)	Terdapat lembaga keuangan mengandung risiko kejahatan yang lebih tinggi dibanding lembaga lain.	Faktor kejahatan pada perbankan berpengaruh pada nasabah.	
8.	(Sri Maharsi & Fenny Fenny, 2006)	Beberapa bank perlu mengetahui faktor loyalitas nasabah agar nasabah tetap loyal terhadap internet banking.	Faktor bank memiliki lebih banyak informasi daripada nasabah adalah agar bank dapat memberikan informasi lebih cepat.	Tidak ada dampak dan cara mengatasi masalah yang terjadi di bank karena kejahatan siber pada jurnal terdahulu.
9.	(Fldr et al., 2022)	Terdapat tiga alat yang digunakan dalam serangan denial of service dan bagaimana ketiga alat ini bekerja..	Faktor dari cara serangan denial of service.	Tidak ada cara untuk mengatasi serangan denial of service pada jurnal terdahulu.
10.	(Ade Borami Ju et al., 2021)	Terdapat berbagai cara yang digunakan penjahat untuk meretas bank dan	Faktor bagaimana peretasan bekerja di perbankan dan cara kerja	

		bagaimana pelanggan melindungi data pribadi dan melaporkannya ke pihak berwenang jika terjadi peretasan.	peretasan	

HASIL DAN PEMBAHASAN

Kejahatan Siber dalam Perbankan

Cyber crime dalam perbankan marak terjadi dan tak kunjung usai. Kejadian seperti hal demikian mungkin sudah tidak lagi asing lagi di dengar. Seperti apa jenis-jenis kasus *cyber crime* yang marak terjadi di perbankan?

1. Skimming

   Skimming adalah penyalinan informasi yang tidak sah dari strip magnetik ke kartu debit atau kredit dengan maksud untuk mencurinya. Metode *skimming* adalah teknik yang digunakan untuk mencuri informasi nasabah saat bertransaksi di ATM. Tiga alat utama digunakan untuk melakukan kejahatan ini: *skimmer*, *hidden camera*, dan *keyboard*. *Skimmer* digunakan untuk merekam aktivitas nasabah saat menggunakan ATM. Alat ini dapat merekam gambar elektromagnetik pada kartu seseorang saat kartu tersebut dimasukkan ke ATM. *Hidden camera* dan *keypad* digunakan untuk merekam aksi korban saat memasukkan PIN di ATM (Ratulangi et al., 2021).

2. Hacking

   Hacking melibatkan penyerangan program komputer yang dimiliki oleh individu dan bisnis untuk memanfaatkan komputer. Seiring waktu, peretasan sering dianggap sebagai kejahatan. Tindakan ini dibuat dengan cara memasuki sistem komputer orang tersebut tanpa izin. *Hacker* menggunakan keahlian mereka untuk melakukan berbagai kejahatan sosial. Direktur Bank Central Asia, Jahja Setiaadmatja, pernah menjelaskan bahaya penggunaan layanan perbankan elektronik. Saat mendaftar online banking pertama kali, maka harus memasukkan nomor ponsel yang akan digunakan untuk mengirimkan kode OTP ke nasabah. Masalahnya adalah banyak pelanggan yang sering mengganti nomor teleponnya, dan jika tidak hati-hati, mereka bisa jatuh ke tangan yang salah. *Hacker* dapat menggunakan nomor ponsel ini untuk berkomunikasi melalui perbankan elektronik, mengirim kode OTP ke peretas dan membobol rekening bank elektronik (Ade Borami Ju et al., 2021).

3. Malware

   Malware (*malicious software*), yaitu software yang tidak diinginkan pada sistem komputer yang sering digunakan untuk mencuri data yang dapat merusak sistem komputer. Malware sulit dideteksi pada sistem komputer. Ada dua cara untuk menyebabkan sistem komputer terkena malware: melalui drive USB dan melalui internet. Sistem komputer yang terinfeksi malware dari drive USB seringkali tidak memiliki fitur keamanan seperti perangkat lunak antivirus, sehingga malware yang terpasang di drive USB dapat dengan mudah masuk ke komputer. Sistem komputer terinfeksi melalui internet, yaitu saat pengguna membuka pesan atau situs web internet. Email yang berbahaya sering dianggap sebagai spam secara langsung oleh sistem, tetapi hanya sebagian kecil dari email ini yang berakhir di kotak masuk. Malware dijalankan dengan mengklik email yang terinfeksi, dan ketika sistem komputer terinfeksi malware, informasi pribadi termasuk informasi perbankan tersimpan dalam komputer (Faridi, 2018).

Dampak DoS pada Perbankan

Menurut (Siregar, 2013), salah satu dampaknya adalah menghabiskan *resources*. Pada dasarnya, layanan akan menggunakan sumber daya yang cukup untuk *hang*, sehingga gagal karena kurangnya *resources* pada komputer yang diserang. Beberapa jenis *resources*

diantaranya: (1) Bandwidth; (2) Kernel Tables - Serangan pada kernel tables dapat menimbulkan hal yang buruk bagi sistem. Kernel memiliki kernel map limit. Saat sistem mencapai keadaan ini, sistem tidak dapat lagi mengalokasikan memori untuk kernel dan akan memulai ulang sistem. (3) RAM - Serangan Denial of Service menghabiskan banyak RAM dan memerlukan restart. (4) Disk - Sebagian besar serangan konvensional dilakukan dengan mengisi daya disk. (5) INETD - Jika INETD gagal, semua layanan melalui INETD akan berhenti bekerja. Informasi konfigurasi rusak atau dimodifikasi.

Lembaga keuangan lebih rentan terhadap kejahatan dari pada lembaga lain. Meningkatnya jumlah nasabah yang menggunakan layanan perbankan online dapat memberikan peluang bagi pelaku kejahatan siber untuk melakukan kejahatan terhadap nasabah. Saat kita hidup di era digital, semakin banyak orang yang menggunakan keahliannya untuk menggunakan teknologi, dan banyak yang menyalahgunakannya (Hidayatullah, 2023).

Cara Mengatasi Serangan DoS di Perbankan

Menurut (Pratama et al., n.d.), serangan DoS dapat ditangani dengan cara-cara berikut:

1. Software
   a. Firewall IPS (Intrusion Prevention System)

      Saat melakukan IPS jaringan, ia memindai lalu lintas jaringan masuk dan keluar yang melewatinya untuk mencari ancaman keamanan. Ketika IPS mendeteksi serangan, ia mencegah atau menolak paket data berbahaya untuk mencegahnya mencapai tujuan. Di sisi lain, firewall adalah mekanisme aturan yang memeriksa header, alamat sumber, alamat tujuan, jenis port, dan alamat tujuan. Jika paket melanggar aturan firewall, paket akan dibuang. Ada yang disebut Next Generation Firewalls (NGFW). Ini memungkinkan satu perangkat untuk bertindak sebagai firewall tradisional, sementara IPS menyediakan beberapa perlindungan DoS untuk mengurangi serangan DoS. Keuntungan firewall dan perangkat IPS adalah mudah dikelola dan digunakan.

   b. Platform Berbasis Software IDS (Intrusion Detection System)

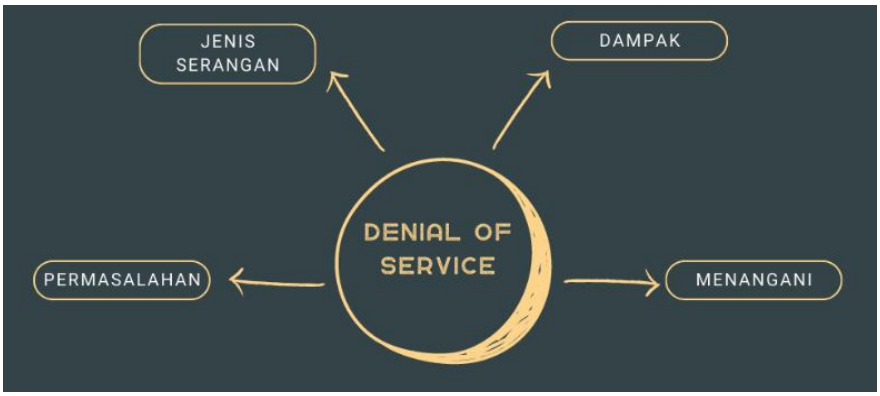
      Jika IPS adalah penjaga keamanan yang bertindak terhadap ancaman yang masuk, IDS dapat dianggap sebagai sistem keamanan untuk bangunan. Layanan manajemen data investasi yang dikelola oleh IDS didasarkan pada platform di mana IDS adalah keamanan pasif. Tidak perlu memiliki jaringan IDS untuk mendeteksi ancaman. Artinya, IDS tidak berada di jalur data yang masuk. Sebaliknya, perangkat IDS terletak di luar jaringan dan saluran datanya tidak teratur. Oleh karena itu, sistem ini tidak memerlukan akses langsung ke data, melainkan menggunakan perangkat pemantauan eksternal yang disebut Test Access Point (TAP) untuk memverifikasi salinan data yang masuk.

      IDS juga dapat memantau paket data yang mencurigakan di berbagai lokasi di jaringan. Mendokumentasikan biaya terhadap risiko yang teridentifikasi. Tujuannya adalah untuk mendeteksi dengan benar lalu lintas berbahaya sebelum meninggalkan jaringan. IDS memungkinkan insinyur keamanan untuk memantau seluruh jaringan tanpa memblokir lalu lintas jaringan. Ketika digunakan dengan benar, alat IDS melindungi dari berbagai ancaman, seperti pelanggaran kebijakan, pengungkapan informasi, kesalahan konfigurasi, dan klien, server, dan perangkat lunak aplikasi yang tidak sah. Semua ini, selain perlindungan terhadap virus tradisional dan serangan Trojan-horse.

2. Hardware
   a. Performa tinggi dan biaya rendah: Pemulihan DoS membutuhkan banyak daya dan sumber daya energi. Untuk melindungi dari serangan DoS, semua paket harus dicegat dan dianalisis tanpa dikompromikan.
   b. Analisa perilaku secara mendalam: Kecanggihan serangan DoS Modern. Satu serangan dapat menghasilkan ribuan tautan atau banyak pola, yang mengakibatkan perilaku aneh seperti membaca file gambar yang sama berkali-kali.
   c. Keamanan yang tak tertandingi: Solusi perlindungan DoS berbasis perangkat keras tidak dapat dideteksi pada jaringan aman. Itu juga dapat menangani lalu lintas yang padat ke titik di mana ia tidak dapat disalahgunakan.

Kerangka berpikir

Pada conceptual framework, hal ini telah didasari oleh perumusan masalah, kajian teoritis, dan riset terdahulu yang signifikan dan pokok bahasan pengaruh peran antar variable. Maka dari itu, dapat diperoleh kerangka konseptual seperti dibawah ini:



Gambar 1: Conceptual Framework

KESIMPULAN

Dari beberapa penelitian terdahulu mengenai dampak Denial of Service pada perbankan, maka penulis dapat mengambil kesimpulan bahwa serangan Denial of Service (DoS) berdampak signifikan terhadap industri perbankan Indonesia. Serangan-serangan tersebut dapat mengganggu layanan perbankan online, menimbulkan masalah bagi nasabah dan merusak kepercayaan masyarakat terhadap sistem perbankan. Selain itu, serangan DoS dapat menyebabkan kerugian finansial yang signifikan bagi industri perbankan, seperti kehilangan dana dan biaya pemulihan sistem yang terkena dampak penyerang. Serangan ini dapat merusak reputasi perusahaan dan berujung pada sanksi dari regulator.

Untuk mengatasi serangan DoS, lembaga perbankan harus memiliki langkah-langkah keamanan tingkat lanjut dan secara teratur menguji keamanan. Hal ini penting untuk memastikan sistem online banking tahan terhadap serangan DoS dan tetap berfungsi melayani nasabah. Selain itu, nasabah harus mewaspadai serangan DoS dan berhati-hati, seperti menghindari akses ke layanan perbankan online menggunakan jaringan yang tidak aman dan kata sandi yang kuat dan unik.

REFERENSI

Ade Borami Ju, Angel Tng, Nadia Carolina Weley, and Hari Sutra Disemadi. “Perlindungan Nasabah Dalam Penerapan Electronic Banking Sebagai Bagian Aktifitas Bisnis Perbankan Di Indonesia.” *Jurnal Perspektif Administrasi Dan Bisnis* 2, no. 1 (2021): 27–40.

Afikah, Nur, and Chairul Mukmin. "Analisa Perbandingan Kinerja Router Terhadap Variasi Serangan Ddos." *Bina Darma Conference On Computer Science* 4, no. 1 (2022).

Chandra, Joko Christian, Program Studi, Manajemen Informatika, Fakultas Teknologi Informasi, and Universitas Budi Luhur. "Proceeding SENDIU 2021 MODEL FRAMEWORK UNTUK ANALISIS KEAMANAN DARI SERANGAN DENIAL" (2021): 978–979.

Faridi, Muhammad Khairul. "KEJAHATAN SIBER DALAM BIDANG PERBANKAN" 1, no. 2 (2018): 57–61.

Fldr, Menggunakan, D A N Raven-storm, Manik Mahardika, I Made Edy Listartha, Gede Arna, and Jude Saskara. "ANALISIS KELAYAKAN TOOLS DENGAN METODE PENYERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS)" 6, no. 2 (2022): 278–285.

Hidayatullah, Cahyo. "Jenis Dan Dampak Cyber Crime." *Prosiding SAINTEK: Sains dan Teknologi* 2, no. 1 (2023): 216–221. https://www.jurnal.pelitabangsa.ac.id/index.php/SAINTEK/article/view/2159.

Pencurian, Abstrak, Bank Indonesia, Rancangan Undang-undang Perlindungan, Data Pribadi, and Bank Indonesia. "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia) Aditama Candra Kusuma , Ayu Diah Rahmani Fakultas Hukum , Universitas Pembangunan Veteran Jakarta Kemajuan Teknologi Sangat Membantu Manu" 5, no. 01 (n.d.): 46–63.

Pratama, Salsyabila Putri, Universitas Airlangga, Mulyorejo Surabaya, Cyber Crime, and Keamanan Komputer. "Memahami Serangan DDoS (Distributed Denial of Service) Dan Pengaruhnya Di Sektor Perbankan" (n.d.).

Ratulangi, Christian Henry, Dr. Anna S. Wahongan, and Franky R. Mewengkang. "Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan." *Lex Privatum* IX, no. 5 (2021): 179–187.