Mempersiapkan diri dari serangan denial-of-service dan menanggapinya

Pertama kali diterbitkan: September 2011
Terakhir diperbarui: Maret 2025

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

Pendahuluan

Publikasi ini dikembangkan oleh Australian Signals Directorate (ASD) bekerja sama dengan Pusat Keamanan Siber Nasional Selandia Baru (NCSC-NZ), Akamai Technologies Ltd dan Cloudflare Pty Ltd, sebagai respons terhadap tren peningkatan serangan penolakan layanan (DoS) di wilayah kami. Dokumen ini menawarkan panduan kepada organisasi tentang mitigasi praktik terbaik berdasarkan keterampilan perdagangan ancaman kontemporer, untuk mempersiapkan dan menanggapi serangan DoS.

Kami menyarankan Anda membaca saran ini bersama dengan publikasi ASD tentang *Perangkat Internet of Things* dan *Amankan Wi-Fi dan router Anda*. Publikasi-publikasi tersebut membantu individu untuk menghindari kontribusi yang tidak disengaja terhadap serangan DoS yang dapat berdampak kepada orang lain.

Serangan DoS adalah serangan siber yang dirancang untuk mengganggu atau merusak layanan daring seperti situs web, email, dan layanan Domain Name System (DNS), guna menolak akses bagi pengguna yang sah. Hal ini biasanya dilakukan dengan membanjiri layanan daring dengan data, koneksi, atau permintaan untuk membanjiri layanan dan menurunkan fungsinya.

Serangan DoS biasanya memerlukan lalu lintas jaringan dalam jumlah besar agar berhasil. Serangan ini menjadi semakin umum, sebagian karena peningkatan jumlah perangkat Internet of Things (IoT) yang mudah disusupi. Karena produsen IoT sering kali memprioritaskan pengalaman pengguna daripada keamanan siber, perangkat yang rentan dapat mencakup barang-barang rumah tangga biasa yang terhubung ke internet seperti TV pintar, ketel, penyedot debu, dan sistem keamanan. Perangkat ini sering kali dapat disusupi dari jarak jauh oleh pelaku kejahatan untuk membuat 'botnet' perangkat yang menghasilkan lalu lintas jaringan ini, yang dapat mengakibatkan rumah tangga dan organisasi secara tidak sengaja berkontribusi pada infrastruktur yang memungkinkan terjadinya serangan DoS.

Aktivitas terkini menunjukkan bahwa setelah pelaku kejahatan berhasil membobol sejumlah besar perangkat IoT, mereka dapat menyewakan atau menjual infrastruktur ini kepada penjahat dunia maya dan aktivis peretas, yang semakin tertarik untuk melakukan serangan DoS terhadap target yang mereka pilih. Dalam sebagian besar kasus, serangan DoS dilakukan untuk menyebabkan kerugian finansial dan produktivitas organisasi, atau untuk mendapatkan perhatian publik atas suatu tujuan. Contoh aktivitas ini dijelaskan dalam nasihat ASD *Pelaku kejahatan yang terkait dengan Republik Rakyat Tiongkok meretas router dan perangkat IoT untuk operasi botnet botnet (People's Republic of China-linked actors compromise routers and IoT devices fro botnet operations)*.

Seiring dengan semakin digitalnya ekonomi kita dan meningkatnya jumlah perangkat IoT yang tidak aman dan terhubung ke internet, serangan DoS kemungkinan akan terus meningkat.

Untuk mengganggu atau menurunkan layanan daring suatu organisasi, pelaku kejahatan menggunakan sejumlah pendekatan, termasuk:

- mengarahkan sejumlah besar lalu lintas jaringan yang tidak diinginkan ke layanan daring dalam upaya untuk menghabiskan semua lebar pita jaringan (network bandwidth) yang tersedia
- mengarahkan lalu lintas jaringan yang disesuaikan ke layanan daring dalam upaya untuk menghabiskan sumber daya pemrosesan komputer mereka
- menggunakan beberapa komputer, perangkat IoT, atau perangkat lain yang terhubung ke internet untuk mengarahkan lalu lintas jaringan ke layanan daring dari berbagai arah dan dalam skala yang jauh lebih besar, jenis serangan DoS umum yang disebut sebagai serangan DoS terdistribusi (DDoS)
- membajak pendaftaran domain atau server DNS suatu organisasi dalam upaya untuk mengalihkan pengguna yang sah dari layanan daring organisasi.

Organisasi tidak dapat menghindari menjadi sasaran serangan DoS, tetapi ada sejumlah tindakan yang dapat diterapkan organisasi untuk mempersiapkan dan berpotensi mengurangi dampaknya. Mempersiapkan diri dari serangan DoS sebelum terjadi adalah strategi terbaik, karena tanpa persiapan, sulit dan kurang efektif untuk merespons selama serangan DoS.

Meskipun organisasi terutama berfokus pada perlindungan diri dari serangan DoS, mereka juga harus mengambil langkah-langkah untuk mencegah layanan daring dan perangkat yang terhubung ke internet disalahgunakan oleh pelaku kejahatan untuk menargetkan orang lain.

Mempersiapkan diri dari serangan DoS

Dalam konteks meningkatnya volume serangan DoS di seluruh wilayah kami, sebelum menerapkan langkah apa pun untuk mempersiapkan diri dari serangan DoS, organisasi Anda harus terlebih dahulu menilai kebutuhan bisnisnya untuk menentukan apakah setiap layanan daring Anda harus tetap beroperasi selama serangan DoS, atau apakah gangguan layanan sementara dapat diterima.

Jika organisasi Anda ingin meningkatkan kemampuannya untuk menahan serangan DoS, Anda harus secara proaktif menerapkan langkah-langkah berikut, jika sesuai dan praktis, sebelum serangan DoS terjadi.

- Jika organisasi Anda menggunakan jaringan pengiriman konten (CDN), Anda harus menerapkan langkah-langkah tambahan berikut, jika sesuai dan praktis.
  - Pertimbangkan untuk menggunakan CDN yang mencakup fungsionalitas untuk melindungi server web asal Anda dari berbagai serangan lapisan aplikasi dan jaringan – beberapa CDN mungkin menyertakan fitur-fitur ini sebagai bagian dari firewall aplikasi web di tepi.
  - Hindari pengungkapan publik yang tidak perlu atas alamat Protokol Internet (IP) server web asal Anda, dan pastikan bahwa setiap paparan publik dilindungi dari serangan DoS.
  - Hindari penggunaan alamat IP untuk server web asal yang dapat diprediksi oleh pelaku kejahatan, misalnya, alamat IP dalam subnet jaringan yang sama dengan alamat IP yang diungkapkan ke publik dari layanan daring Anda.
  - Gunakan kontrol akses jaringan (seperti firewall) untuk memastikan bahwa hanya CDN dan jaringan manajemen resmi organisasi Anda yang dapat mengakses server web asal Anda.
  - Pertimbangkan untuk menggunakan konektivitas jaringan beragam yang tangguh, yang mungkin mencakup konektivitas jaringan privat, antara server web asal dan penyedia CDN Anda, jika Anda memerlukan tingkat perlindungan yang lebih tinggi untuk server web asal Anda.
  - Konfigurasikan CDN, server web asal, dan header HTTP klien untuk mengoptimalkan jumlah caching yang dilakukan.
  - Pertimbangkan untuk mempartisi server web asal sehingga permintaan dari alamat IP berisiko rendah ditangani secara terpisah dengan permintaan dari alamat IP berisiko tinggi, jika Anda memerlukan tingkat ketersediaan yang lebih tinggi.

- Tentukan fungsionalitas dan kualitas layanan apa yang dapat diterima oleh pengguna sah layanan daring Anda, cara mempertahankan fungsionalitas tersebut, dan fungsionalitas apa yang tidak diperlukan selama serangan DoS.
- Peroleh dan gunakan layanan mitigasi serangan DoS berbasis cloud.
- Pertimbangkan untuk mengurangi permukaan serangan organisasi Anda dengan:
  - mengalihdayakan layanan daring dasar (seperti DNS) ke penyedia layanan bereputasi baik yang mampu menahan serangan DoS
  - memisahkan layanan daring penting (seperti email) dari layanan daring lain yang lebih mungkin menjadi target (seperti situs web)
  - memastikan bahwa layanan mitigasi serangan DoS hanya mengizinkan lalu lintas jaringan yang terkait dengan port jaringan layanan daring tersebut.
- Diskusikan dengan penyedia layanan Anda mengenai detail strategi pencegahan dan mitigasi serangan DoS mereka, khususnya:
  - kemampuan yang terbukti untuk menahan serangan DoS dari seluruh dunia
  - riwayat yang teruji dalam menangani serangan DoS dan pengujian serangan DoS resmi yang komprehensif
  - kemampuan untuk secara otomatis memitigasi sebagian besar jenis serangan DoS tanpa keterlibatan manusia, seperti analisis manual lalu lintas jaringan
  - pendekatan untuk menentukan harga layanan mereka, seperti apakah biayanya tetap atau bervariasi berdasarkan jumlah lalu lintas jaringan dan sumber daya pemrosesan komputer yang digunakan, dan apakah Anda dapat menetapkan batas penagihan
  - ambang batas untuk memberi tahu Anda atau menonaktifkan layanan daring mereka selama serangan DoS
  - tindakan yang telah disetujui sebelumnya yang dapat dilakukan selama serangan DoS
  - pengaturan pencegahan serangan DoS dengan penyedia hulu.
- Terapkan langkah-langkah untuk mendeteksi serangan DoS, seperti pemantauan waktu nyata dan pemberitahuan ketersediaan sistem, lalu lintas jaringan, sumber daya pemrosesan komputer, dan biaya terkait.
- Siapkan versi statis situs web Anda yang memerlukan pemrosesan dan bandwidth minimal untuk memfasilitasi kesinambungan layanan selama serangan DoS.
- Dapatkan dan gunakan layanan daring yang sangat tangguh dengan bandwidth besar, sumber daya pemrosesan komputer yang memadai, lokasi hosting yang tersebar secara geografis, dan pembersihan lalu lintas berbasis cloud untuk membuang lalu lintas jaringan yang tidak diinginkan – ini biasanya termasuk menggunakan CDN yang memiliki reputasi baik untuk menyimpan konten situs web statis dan melindungi server web asal Anda dari lalu lintas jaringan yang tidak diinginkan.
- Lindungi nama domain organisasi Anda dengan menggunakan penguncian pendaftar, mengonfirmasi detail kontak pendaftaran domain dan detail lainnya sudah benar, serta mengikuti panduan tambahan yang diuraikan dalam publikasi ASD *Keamanan Sistem Nama Domain untuk pemilik domain*.
- Pertahankan detail kontak terkini untuk penyedia layanan Anda dan bagikan detail kontak organisasi Anda dengan mereka, pastikan semua kontak tersedia berdasarkan keperluan organisasi Anda, misalnya, 24 jam sehari, 7 hari seminggu.
- Berikan detail kontak organisasi Anda di luar jaringan untuk saluran komunikasi tepercaya kepada penyedia layanan Anda, untuk saat saluran komunikasi normal gagal.
- Kembangkan, terapkan, dan pelihara rencana respons insiden keamanan siber, yang mencakup berbagai jenis serangan DoS terhadap setiap layanan daring Anda yang diperlukan untuk menahan serangan DoS, dan menjalankan rencana tersebut setidaknya setiap tahun.

- Arsitektur aplikasi untuk melindungi fungsionalitas yang sering disalahgunakan yang menghabiskan lebih banyak sumber daya pemrosesan komputer atau yang menimbulkan biaya finansial tambahan (seperti mengirim pesan SMS).
  - Perlindungan mencakup pembatasan kecepatan dan verifikasi bahwa permintaan berasal dari manusia.
  - Lakukan pengujian serangan DoS termasuk menargetkan alur logika yang tidak tepat dalam fungsionalitas aplikasi.
  - Lakukan pengujian beban yang lebih luas untuk mengidentifikasi dan memperbaiki vektor DoS.

Menanggapi serangan DoS

Jika organisasi Anda belum siap menghadapi serangan DoS, Anda dapat mencoba menerapkan beberapa tindakan di atas selama serangan DoS, meskipun tindakan tersebut mungkin kurang efektif dan memerlukan waktu untuk diterapkan, sehingga mengurangi kemampuan organisasi Anda untuk merespons.

Organisasi Anda harus menerapkan tindakan berikut selama serangan DoS, jika sesuai dan praktis.

- Tetapkan rencana respons insiden keamanan siber Anda.
- Tanyakan kepada penyedia layanan Anda apakah mereka dapat segera menerapkan tindakan responsif – jika Anda belum pernah membahas kemampuan mereka untuk merespons sebelumnya, Anda mungkin menemukan bahwa mereka tidak dapat atau tidak mau merespons, atau mengenakan biaya tambahan.
- Nonaktifkan fungsionalitas yang tidak penting atau hapus konten yang tidak penting dari layanan daring Anda yang membuat serangan DoS saat ini efektif, misalnya, terapkan versi situs web Anda tanpa fungsionalitas pencarian, konten dinamis, atau file besar.
- Pertahankan komunikasi dengan pelanggan Anda dan penyedia layanan Anda, termasuk penyedia layanan mitigasi serangan DoS, dan terus pantau ketersediaan layanan daring Anda.
- Pertimbangkan untuk mengubah alamat IP server web asal Anda jika menjadi target langsung, dan hindari pengungkapan alamat IP baru ke publik tanpa adanya perlindungan.
- Laporkan serangan DoS ke pihak terkait, termasuk ASD dan NCSC-NZ sesuai bagian 'Detail kontak' dari publikasi ini.

Hindari berkontribusi terhadap serangan DoS

Organisasi Anda harus menerapkan langkah-langkah berikut untuk menghindari kontribusi yang tidak disengaja terhadap serangan DoS yang dapat berdampak kepada pihak lain.

- Hindari mengekspos layanan, perangkat IoT, dan perangkat lain yang terhubung ke internet ke internet yang tidak diperlukan, dikonfigurasi secara tidak aman, atau tidak dirawat dengan baik.
- Konfigurasikan, rawat, dan pantau layanan, perangkat IoT, dan perangkat lain yang terhubung ke internet yang terekspos ke internet dengan aman.
  - Panduan tambahan untuk bisnis kecil tersedia dalam publikasi ASD *Perangkat Internet of Things* dan *Amankan Wi-Fi dan router Anda*.

Jika organisasi Anda menjalankan layanan daring, Anda harus menerapkan langkah-langkah tambahan berikut.

- Prioritaskan peninjauan protokol yang diuraikan dalam saran *Serangan Amplifikasi Berbasis UDP* dari Badan Keamanan Siber dan Keamanan Infrastruktur Amerika Serikat (CISA).
- Pantau vektor amplifikasi baru saat diidentifikasi dan amankan layanan daring Anda terhadap vektor tersebut.
- Konfigurasikan kontrol akses jaringan masuk dan keluar untuk membatasi akses ke layanan dan organisasi daring yang sah.
- Blokir akses publik anonim untuk layanan daring yang rawan penyebaran informasi, jika tidak diperlukan.
- Pertimbangkan untuk menerapkan mekanisme pembatasan laju untuk mengurangi konsekuensi penyalahgunaan, jika pemblokiran atau penerapan kontrol akses tidak memungkinkan atau tidak sesuai.

Informasi lebih lanjut

Manual keamanan informasi ASD adalah kerangka kerja keamanan siber yang dapat diterapkan organisasi untuk melindungi sistem dan data mereka dari ancaman siber. Saran dalam *Strategi untuk mengurangi insiden keamanan siber*, beserta Delapan Hal Penting, melengkapi kerangka kerja ini.

Manual Keamanan Informasi Selandia Baru adalah manual Pemerintah Selandia Baru tentang jaminan informasi dan keamanan sistem informasi. Buku ini merupakan panduan praktisi yang dirancang untuk memenuhi kebutuhan para eksekutif keamanan informasi lembaga serta vendor, kontraktor, dan konsultan yang menyediakan layanan kepada lembaga.

Informasi lebih lanjut tentang berbagai jenis serangan DoS tersedia dalam publikasi CISA *Panduan Cepat DDoS* dan *Memahami dan Menanggapi Serangan Penolakan Layanan Terdistribusi*.

Detail kontak

Di Australia, jika Anda memiliki pertanyaan tentang panduan ini *tulislah surat ke ASD* atau hubungi 1300 CYBER1 (1300 292 371).

Di Selandia Baru, untuk melaporkan insiden keamanan siber, kirimkan email ke incidents@ncsc.govt.nz atau kunjungi halaman web NCSC-NZ Laporkan insiden.

Penafian

Materi dalam panduan ini bersifat umum dan tidak boleh dianggap sebagai nasihat hukum atau diandalkan untuk bantuan dalam keadaan tertentu atau situasi darurat. Dalam masalah penting apa pun, Anda harus mencari nasihat profesional independen yang sesuai sehubungan dengan keadaan Anda sendiri.

Persemakmuran tidak bertanggung jawab atau berkewajiban atas kerusakan, kerugian, atau biaya apa pun yang ditimbulkan sebagai akibat mengandalkan informasi yang terkandung dalam panduan ini.

Hak Cipta

Penggunaan lambang Coat of Arms

Persyaratan penggunaan Lambang Coat of Arms diperinci di situs web Department of the Prime Minister and Cabinet Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

Untuk informasi lebih lanjut, atau untuk melaporkan insiden keamanan siber, hubungi kami:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Nomor ini hanya dapat digunakan di Australia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre