National Cyber Security Centre
Ministry of Security and Justice

Continuity of online services

Protect your organisation against (D)DoS attacks

Factsheet FS-2013-01 | version 2.0 | 14 March 2016

The NCSC advises to take both technical and organisational measures to protect your organisation against the various forms of (D)DoS attack. These attacks can disrupt your organisation's ICT and, in turn, any dependent business activities. This can lead to (reputation) damage. (D)DoS attacks constitute a real threat to organisations that provide online services, such as websites.

Make an overview of your ICT infrastructure. Take technical measures to protect in-house components. For external components, make arrangements with the relevant supplier. Prepare your organisation for an attack by creating a clear response and communication strategy.

Target audience

IT managers and others responsible for information security within organisations with online services, such as websites.

This factsheet was written in collaboration with:

The Dutch Tax Authority, Capgemini Infrastructure Services, NaWas (part of NBIP), Schuberg Philis, SURFcert and other domain experts.

Background

During a Denial-of-Service (DoS) attack, online services or the supporting infrastructure is overburdened or overloaded with network traffic. Attackers also abuse software vulnerabilities to cause supporting equipment to become unavailable. These attacks result in the online services becoming inaccessible to your employees or customers. In many cases, this type of attack is carried out by multiple computers, simultaneously. This is referred to as a *Distributed* Denial-of-Service (DDoS) attack. The impact to your organisation is ultimately the same, so this factsheet refers to both types of attack by a single term: **(D)DoS**.

Key facts

1. A (D)DoS attack can disrupt your online services.
2. Attacks are becoming larger and more complex. At the same time it is becoming easier and cheaper to launch attacks.
3. Even small companies, like webshops, can be extorted using the threat of (D)DoS attack.
4. Take technical and organisational measures to make your online services more resilient to attack.
5. Make arrangements with your ICT suppliers regarding their (D)DoS protection.

A (D)DoS attack can take many forms.[1] There are dozens of known attacks that target routing, specific network services or overloading the computational capacity of specific equipment. Nowadays attacks are largely ‘multi-vector’. This means that multiple attack techniques are used simultaneously or after one another during an attack. Attackers sometimes change their tactics during the attack. For instance, blocking one type of attack leads to a different type being launched.

There are several types of attackers that perform (D)DoS attacks.[2] **Hacktivists**, including the hacktivist collective ‘Anonymous’, use (D)DoS attacks to send a political message. **Criminals** use this type of attack to earn money by extorting companies, even small companies. (D)DoS attacks are also employed to conceal other criminal activities. **State actors** use (D)DoS attack to silence opposition. **Script kiddies** use simple tools to carry out attacks, often without a clear motive. **Insiders** carry out attacks for various reasons. Examples include a disgruntled employee or a student attempting to prevent an exam from taking place.

Attackers employ a variety of tools and techniques to hide their identity. As a result, there is generally a small chance of being caught. **IP spoofing** makes it possible to modify network traffic so that it appears to originate from different networks. Attacks are often launched from **botnets**. These networks consisting of a large number of infected computers that are controlled from a central point. Rather than attacking your network directly, attackers also launch **reflective attacks**. This occurs when attackers send requests to several resources, such as DNS servers and uPnP services on modems, using a spoofed IP address. Consequently, the response is sent to the victim. Nowadays, attackers can use **paid (D)DoS services**. These enable attackers to launch large-scale attacks at the push of a button and require little money and no advanced knowledge.

Most of the reported (D)DoS attacks target websites. In principle, every online service is vulnerable to this type of attack.

- Attackers overload applications with bogus requests. Legitimate users can then no longer be served. In addition, attackers send computationally ‘expensive’ requests. An example is loading a webpage that, in turn, has to retrieve a large amount of data from a database. An increasingly popular type of attack is the slow HTTP POST attack. During this attack, the attacker periodically sends incomplete requests to a server. This results in a large number of open connections while the server waits for rest of the request. These attacks are difficult to detect because the requests appear to be legitimate.
- Servers are overloaded with attacks at the network or transport level. An example is the *TCP SYN flood attack* during which a server receives multiple requests to set up a TCP connection. The server reserves the necessary resources for each connection until no resources are left. Legitimate users can then no longer be served.
- Some attacks target the network or network appliances. These attacks often attempt to consume all available bandwidth or processing power of the network appliances. These appliances are also often targeted by the same attacks as servers, such as TCP SYN flood.
- If your application offers a TLS secured connection, it can also be targeted by specific types of attacks. Attackers abuse this functionality to consume a relatively large amount of processing power from the server with relatively little effort.

What is the matter?

A (D)DoS attack can disrupt your organisation’s ICT and, consequently, any dependent business activities. This constitutes a real threat to organisations that provide online services, such as websites, for which continuity is important. Depending on the type of attack, this can even result in your organisation not being able to use ICT systems because they are slow or unresponsive. Due to the disruption of your online services, your customers can no longer be served.

Generally speaking, the chance of catching an attacker is small, whereas, the damage from a (D)DoS attack is quite large. Most organisations see reputational damage as the main point of concern, followed by mitigation costs and lost revenue. In addition, such an attack can prevent an organisation from meeting its contractual obligations. This may, in turn, lead to other problems.

[1] This factsheet focuses exclusively on deliberate attacks. “Natural” factors, such as an abnormally high number of users simultaneously visiting your website, are intentionally disregarded.

[2] More information regarding actors and motives can be found in the Cyber Security Assessment Netherlands: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html

What does the NCSC recommend?

The NCSC advises taking both technical and organisational measures to protect your organisation against the various forms of (D)DoS attack. Discuss the following recommendations with the relevant stakeholders within your organisation, including those responsible for the administration and continuity of your online services.

Recommendation 1: make an overview and monitor your infrastructure

Make an overview of your infrastructure. Which online services does your organisation offer and which platforms and infrastructure do these require? Which of these are vulnerable to a (D)DoS attack? Are there certain services that are more important than others? What is, for instance, the impact to your organisation if a certain service were no longer available? How is your network segmented? Is everything in-house or have some servers or services been outsourced to third-parties? Consider the internet provider and third-party online services on which your organisation relies. Identify the entire supply-chain of your online services so that you can adequately protect them all.

Once you have an up-to-date overview of your infrastructure, establish a baseline of 'normal' behaviour: the amount of website traffic, the usual times, the type of traffic, the ports used and so on. This should be based on a representative period. It is not an average, but rather a range within which network traffic and system behaviour is defined as 'normal'. For in-house infrastructure you can use system logs and statistics from your network appliances. If your organisation has outsourced services to third-parties, you will have to work together with these parties to find solutions.

Once you have established a baseline, you can then begin to monitor incoming and outgoing network traffic. This means automatically checking if periodic measurements significantly deviate from the baseline. Monitoring also makes it possible to analyse the type of (D)DoS attack and the effectiveness of countermeasures. Without a suitable monitoring system it is difficult to distinguish attacks from legitimate traffic or technical failures. Consider predictable deviations from the baseline, such as advertising campaigns or annual events when many legitimate users are expected.

Recommendation 2: check with each of your third-party suppliers to find out which (D)DoS countermeasures are in place and what the relevant contractual agreements are

Use the overview created for Recommendation 1 to check with each of your third-party suppliers about their (D)DoS protection. What is their approach and what are the contractual agreements that cover this subject?

Contact each third-party supplier and verify:

- contact information for individuals that can be called during a (D)DoS attack;
- which countermeasures and support they offer to mitigate attack and what the effects could be. For instance, it might be the case that your hosting provider uses *blackholing/null-routing* during an attack. This will route traffic meant for your website to a 'black hole' in order to protect the rest of their infrastructure;
- which countermeasures they have taken to protect your services from the effects of attacks against other customers that use their services. For instance, if you use shared hosting resources, attacks against the other customers can have a negative effect on your services;
- in the case of shared hosting: with what (type of) customers you share the infrastructure;
- which anti-spoofing mechanisms are used;[3]
- which detection mechanisms are used to detect (D)DoS attacks at an early stage;
- what agreements have been made regarding the installation of security updates;
- if the capacity of your systems and network is sufficient.

Recommendation 3: find out which countermeasures have been taken to protect your in-house infrastructure and take additional steps, if necessary

The NCSC advises taking multiple, overlapping countermeasures to adequately protect your in-house infrastructure from (D)DoS attacks. Use the overview created for Recommendation 1 to make an inventory of the countermeasures that are already in place to protect your in-house infrastructure. For each application, server or network appliance that is not adequately protected, look into the possible countermeasures.

In the factsheet **Technical measures for the continuity of online services** you will find an extensive list of technical measures.[4] Consider taking the measures on this list, if they have not already been taken. Depending on the degree of your ICT outsourcing, some measures cannot be taken without working together with your third-party suppliers.

Recommendation 4: prepare your incident response and think about failover scenarios for your online services

Make a plan to follow during a (D)DoS attack. Describe how an attack will be detected and which steps will be taken. For instance, who will keep track of the timeline and characteristics of the attack? Who will collect the necessary information to file

[3] Internet providers can apply filtering following well-known standards, such as BCP38: http://www.bcp38.info to stop spoofed traffic.

[4] https://www.ncsc.nl/english/current-topics/factsheets/factsheet-technical-measures-for-the-continuity-of-online-services.html

a police report (see box)? Consider setting up a specialized team[5] that can autonomously take action during such incidents.

Think about backup and failover scenarios for your online services. Make arrangements with your third-party suppliers for response mechanisms and possible additional services. An example of this is a simple website that lets your customers know that your organisation is working hard to remedy the situation.

Consider setting up alternative channels of communication to be used during an attack. This enables you to remain in contact with important systems and organisations.

Recommendation 5: prepare a communication strategy

Determine a communication strategy for statements directed at your employees, customers, suppliers, government and other stakeholders. Once an attack has begun, it is too late to decide how communications will be handled. Statements regarding (D)DoS resilience can actually lead to (D)DoS attacks. Ensure that your communications advisor understands the general consequences of an attack. What is being done? How long will it last? Where can people find additional information? Avoid any uncertain or inaccurate statements.

Filing a police report

Launching a (D)DoS attack is a criminal offense that is punishable with imprisonment or fines. It is important to file a police report. Even if the perpetrator cannot be caught, filing a report helps to give a better picture of the extent of this phenomenon.

If you choose to file a report, call 0900-8844 to make an appointment with your local police department. Request that a digital expert is present during this appointment. Bring the relevant attack information from your monitoring system.[6]

[5] Examples include a Security Operations Centre (SOC) or a Computer Security Incident Response Team (CSIRT).

[6] See the factsheet 'Technical measures for the continuity of online services' for an overview of relevant attack information: https://www.ncsc.nl/english/current-topics/factsheets/factsheet-technical-measures-for-the-continuity-of-online-services.html

Publication
Nationaal Cyber Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2013-01 | version 2.0 | 25 April 2016

This information is not legally binding.