[TLP:WHITE]

# Good practices in DDoS countermeasures

**Warszawa**
**February 2022**

# Table of Contents

# I. Introduction

Modern organization operating in a modern and dynamic business environment relies heavily on the digital domain, where it should operate in a secure manner, but also maintain confidentiality, integrity and accessibility.

One of the popular cybercriminal activities which target availability are *Denial of Service* (DoS) and *Distributed Denial of Service* (DDoS) attacks)[1].

Simply speaking, DDoS attacks can be described as attacks that cause temporary unavailability of ICT systems and services that the Organization provides via digital domain. DDoS attacks which directly affect accessibility, often have a negative data integrity and confidentiality impact, thus greatly increase risk of data loss for the Organization.

The lack of accessibility caused by DDoS attacks can cause factual adverse impact on Organization, such as:

a) significant financial losses due to interruption of business operations and follow-up claims by customers and external suppliers, service users, etc.;
b) reputational damage from temporary failure to provide services to business and individual customers;
c) breach of legal regulations;
d) other, unspecified risks related to unaaccessibility of services.

Unaccessibilty of services of an Organization (or in the extreme case of several or more Organizations from one or more sectors of the economy) which as a result of an attack will not be able to provide its services, may also have a significant negative impact on the overall socio-economic situation in the country if the Organization provides:

a) provides public services to citizens;
b) is a public trust institution;
c) provides so-called basic need services;
d) core public services;
e) services for a wide range of other Organizations which perform the above tasks (chain of supply);
f) services for key players responsible for broadly understood safety and security.

Level of sophistication and effectiveness of DDoS attacks has increased dramatically, and has often become a part of CaaS (*Cybercrime as a Service*) model offered by criminals. Off-the-shelf services, which allow to carry out DDoS attacks, are available not only in DarkNet, but also directly on the Internet, e.g., advertised on Youtube channels or on Reddit. According to predictions of DDoS global analytical centers, their scale will keep growing due to such

[1] For simplicity, the term DDoS is used hereafter

developments as 5G technology. 5G makes possible to connect new devices to the Internet and opens gates for wide adaptation of so-called *Internet of Things* (IoT) with, consequently, many more devices connected to IP network). Other developments include wider adaptation of fiber optic networks for end users, and general increase in number and bandwidth of Internet connections of end users.

According to statistics in the 2019 ENISA report[2] dated 2019:

- total number of DDoS attacks in Q3 2019 (compared to the same period in 2018) increased by 241%;
- 79.7% of all DDoS attacks were SYN-Floods;
- 86% of mitigated attacks in Q3 2019 used more than two vectors;
- 84% of DDoS attacks lasted less than 10 minutes
- the longest DDoS attack in Q2 2019 lasted 509 hours.

The following are sample statistics on the growing scale of DDoS attacks published by:

a) A10, for Q1 2021. (scale in millions)

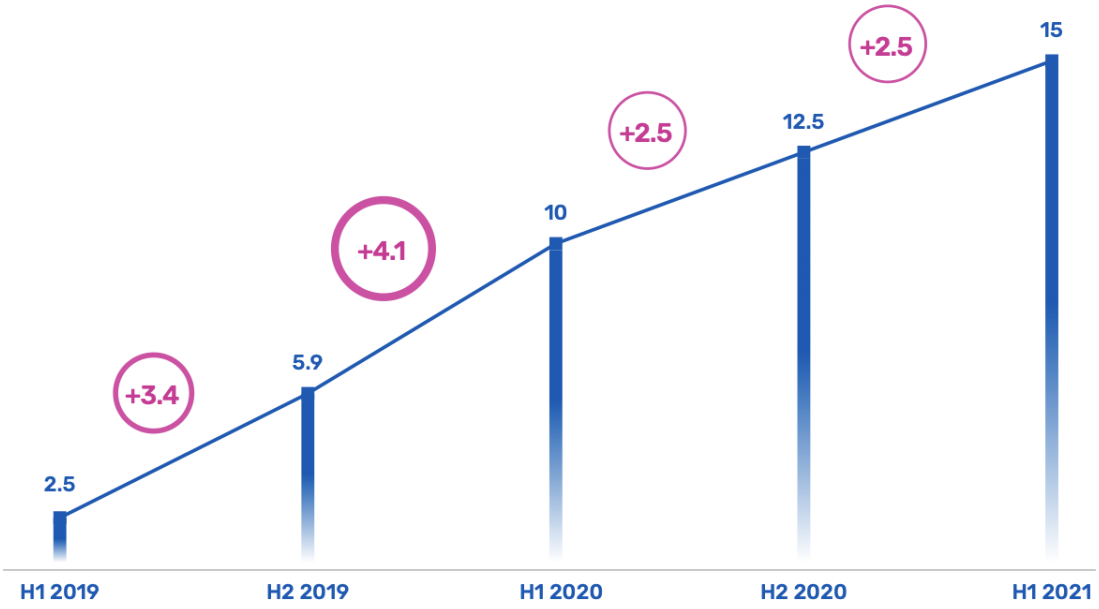


Fig 1 – DDoS attacks growth from 2019 to 2021. Source[3].

b) Kaspersky, which compares the scale of DDoS attacks between Q4 2020 (taken as 100%) and Q3 and Q4 2021, which shows increases from ~250 to ~500%

[2] Source: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service
[3] Source: https://www.a10networks.com/wp-content/uploads/A10-EB-ddos-attack-mitigation-a-threat-intelligence-report.pdf

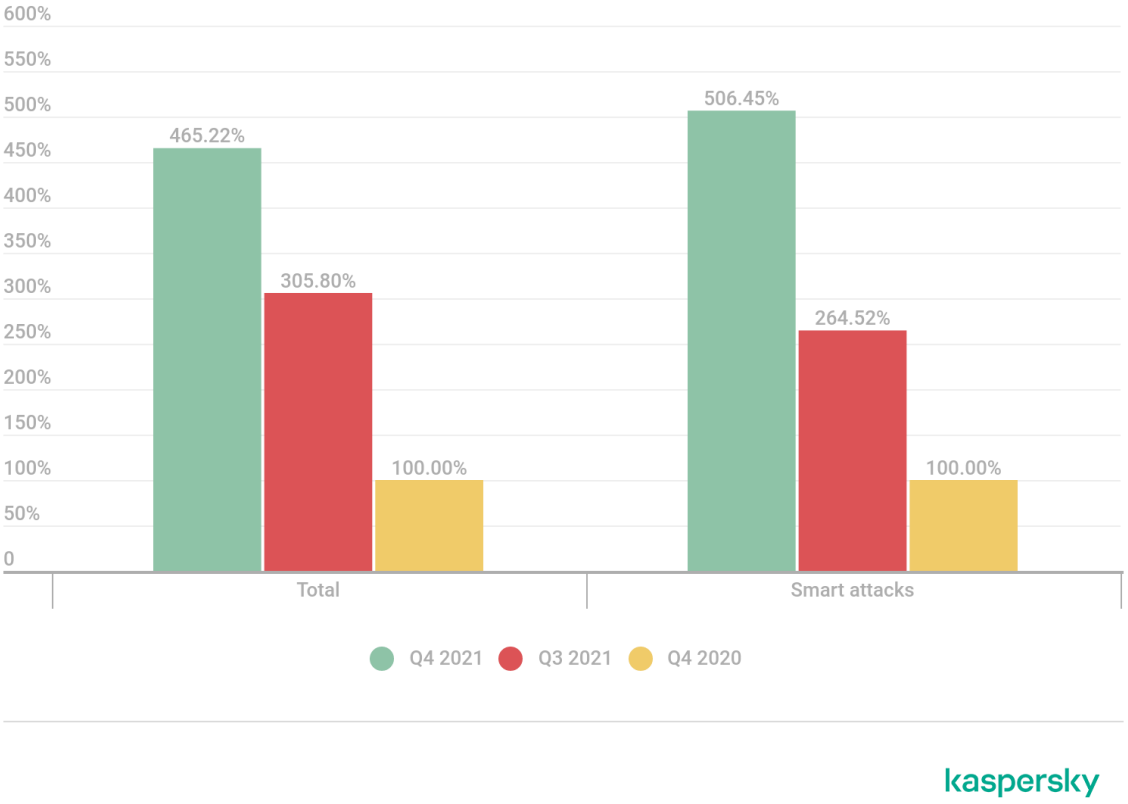


Fig 2 - increase in scale of DDoS attacks Q4 2020 - Q3, Q4 2021. Source[4].

DDoS attacks are becoming not only a tool for cybercriminals (understood as cybercriminal gangs) focused on financial gain[5], but they are also used by the so-called *state-sponsored hackers*, i.e., hacking groups operating within the structure or on behalf of particular states.

As a real, offensive weapons operating in cyberspace, they become an element of pressure and direct influence in geopolitical games.

The study, following by the above introduction is the result of the work of specialists in the field of telecom and cyber-security and presents a set of good practices combined with solution concepts for telecom architecture, which should be thoroughly analyzed by every Organization.

For practical reasons, the study does not include characteristics of types of DDoS attacks – all necessary information is publicly available on the Internet, and actions of cyber criminals in this area are constantly evolving, which, in short term, would make the study outdated.

Concepts, tools and techniques presented in the study to protect against DDoS attacks are intentionally not assigned to specific types of attacks, because, using one of those solutions often provides protection against different types of DDoS attacks.

[4] Source: https://securelist.com/ddos-attacks-in-q4-2021/105784/
[5] Source: https://www.proofpoint.com/us/blog/threat-insight/ransom-ddos-extortion-actor-fancy-lazarus-returns

Every Organization should perform risk assessment related to DDoS attacks on its computer infrastructure, and on the basis of results of that analysis, choose appropriate tools (including those from the list below), technical solutions, or optimal model of Internet access architecture, in order to protect against DDoS attacks.

## II. DDoS attack countermeasures

The following list is not complete, but it can be an indication of what components should be considered when strengthening the resilience of an organization's infrastructure against attacks, or when performing a risk assessment for organization's state of readiness in particular areas.

### 1. Active routing management

On the Organization's side, the link to the Internet should be organized through a dedicated Internet access node via BGP protocol with a fixed (defined and described in a dedicated document) peering policy/policy for exchanging IP traffic with the outside world.

This can enable and document an informed routing path selection based on the local Internet map. For each Organization, routes to the Internet look slightly different and it is necessary to make decisions on how to exchange traffic by using native BGP protocol mechanism, e.g.,:

a) for outgoing traffic *local pref* and *community*;
b) for incoming traffic *prepend* and *community*. For redundant links to the same telco operator, optional control of the incoming traffic via *MED* metrics can be used, with possibility of propagating prefixes with a mask longer than /24 to distribute the traffic between redundant devices on the Organization's side.

However, the most important thing is to choose the right set of telco operators and local peerings, in particular, in traffic exchange nodes.

MD5 authentication (keys) should also be used for BGP sessions between the Organization and telecom operators which significantly reduces the risk of attacks (e.g. BGP hijacking) or configuration error.

The use of RPKI ROA for the Organization's address space will further protect the Organization from attempts to hijack routing paths. It is also critical to maintain up-to-date records in the RIPE-DB database. It is also recommended to consider mechanisms to automate RIPE-DB database updates.

Filters in BGP configuration should be implemented to reduce the risk of injecting invalid routes into routing path.

In order to minimize the risks associated with routing area, reviewing the set of best practices described as "*Mutually Agreed Norms for Routing Security*"[6] is recommended.

[6] Source: https://www.manrs.org/

## 2. WAN-to-Internet: connection architecture

Correctly described and implemented architecture of Internet connection is the most significant part of strengthening resilience against DDoS attacks for every Organization. Proper implementation provides a significant increase in network infrastructure resistance to attacks. Secure architecture also provides response mechanisms in case of threats that exceed capacity and capability threshold to accept traffic over links.

To ensure higher resilience against DDoS attacks, first of all, it is necessary to multiply the links between the Organization and the Internet. Diversification should include both ordinary technological redundancy (more than one physical connection), as well as redundancy by means of employing multiple service providers to serve the Organization. This offers protection not only against failures of technology, but also against single telecom operator network breakdowns as well as financial or business turbulence. An organization should therefore have links provided by more than one telecom operator, and as far as possible not under the same capital or technology umbrella.

It is also worth considering a process of assessment of the quality of the operator's services, particularly: operator's network backbone capacity, number of end users, network traffic volume, throughput overhead on inter-operator and international links, type and quality of applied security mechanisms, operator's approach to cyber-security issues, and finally the presence of modern technological solutions across the operator's network, such as *scrubbing center* or CDN, mentioned later in this study.

Internet access node must accommodate for different types of links, balancing the advantages and disadvantages of each of the available types. The optimal configuration of Internet access will therefore involve the coexistence of different types of links, so that the organization's communication needs are satisfied in total – we can imagine a node, in which, beside the duplicated international link, there are 2-3 links from national (domestic) operators and connection to two independent nodes exchanging inter-operator traffic, through which CDN networks are also available. This is optimal, as it provides the most cost-effective model, quality and parameters for end users, as well as real resilience against DDoS attacks.

The links used by the Organization as links to the Internet should be divided into:

a) Links for international data traffic (general transmission);
b) Links domestic data traffic (domestic transmission);
c) Peering links dedicated to domestic traffic (peering) and direct peering links (local direct peering - as a subclass of peering links);
d) Resource links (including CDNs).

| | **Cost** | **Bandwidth** | **Hop count** | **Latency** | **Number of users (availability)** | **Probability of successful DDoS attack** | **Priority** |
|---|---|---|---|---|---|---|---|
| **International transmission link** | Relatively high | Limited | Very high | High | All Internet | Very high | 4 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **National transit / transmission link** | Relatively high | Limited | Medium | Medium | National (whole country) | Negligible | 3 |
| **Domestic peering link** | Low | Very high | Zero | Negligible | Limited to participants in traffic exchange nodes | Negligible | 2 |
| **Resource link** | Low | Very high | Zero | Negligible | None | Zero | 1 |

Tab 1 - Summary of general characteristics of Internet access links. Source: own study

The above table summarizes characteristics for different link types, with particular focus on features useful for their selection in Internet access nodes in the Organization.

Different types of links offer different parameters, e.g.:

1) **Cost** - measured as the amount of PLN per each available gigabit of bandwidth;
2) **Throughput** - measured as the capacity obtainable for the Organization on a link of a given type, while maintaining reasonable costs of acquiring such a link;
3) **Hop count** - measured as the number of AS available through a link of a given type and the average path length (AS-path) when accessing a given resource; the shorter the average path length to resources or users, the more reliable the link and the better its parameters
4) **Latency** - average delay (in ms) between the Organization and the user or resource;
5) **User count** - the range of a given link understood as the number and type of resources available through a link of a given type;
6) **Probability of DDoS attack** - understood as the probability that a successful attack will occur over a link of a given type, with the volume / intensity that actually threatens the stability of the Organization
7) **Priority** - understood as a recommended routing order, if a given resource is accessible over more than one route - the lower the value, the more preference for the route.

The types of links:

**a) International transmission link**

International (trans-national) transit / transmission link is used to communicate with all users and services available on the Internet. These links are characterized by relatively high cost per 1 gigabit of bandwidth and limited throughput (in terms of maximum speed of a single TCP session). The average BGP and traceroute path is the longest, which negatively affects reliability (potential failures of intermediate nodes multiplied by the number of nodes) and latency (generated by intermediate nodes). This link typically experiences high latency in ms. This link can take over all the traffic from any other type of link described in the table (the so-called last resort backup). Because of the characteristics of this link, it is the most vulnerable to the probability of a successful DDoS attack of volumetric nature.

This link should be used to communicate with the outside world as the lowest priority link – to handle traffic that does not travel via other types of links, mainly traffic from abroad and as a last resort backup.

In case of extremely powerful DDoS attacks, temporary disabling of international transit / transmission restores availability of services for domestic customers and can be treated as the last element of reaction to a massive DDoS attack.

**b) National transit / transmission link**

It is used for communications for all users of a given country. This type of link is characterized by a relatively high cost per 1 gigabit of bandwidth and slightly higher throughput than international transit / transmission links. Domestic transit / transmission links have relatively short BGP and traceroute paths (no more than a few intermediate nodes), which has a positive effect on reliability and quality of transmission for this link type. Average latency is counted in single milliseconds. Because of the characteristics of this link, i.e. providing the Organization with traffic from Internet users in a given country, it is only marginally exposed to DDoS attacks, due to an extremely limited number of Internet users in an average-sized country compared to the worldwide Internet audience, and a known location of the users (geographically limited to the area of a given country). Number of hosts which are potentially a part of any botnet, that can be used for DDoS attacks through that link is negligible versus number of hosts located in the global Internet, what greatly reduces probability and scale of such attack.

Traffic on that link is crucial for servicing Internet users in a specific country – over 90% of traffic may go through that link (unless the user is available through peering link – see information below).

In practice, this means that cutting off all other telecom links (due to technological failure or a successful DDoS attack on an international transit / transmission link) will not significantly disrupt services provided by the organization to users in in a given country.

The key feature of this type of link is also the fact that the state services, through cooperation with telecom operators, are always able to reach the end user who generates the traffic (which ensures lack of anonymity and full attribution).

This link should be used to communicate with domestic users, as long as these users are not available on the peering link.

**c) Peering Links (IX)**

Used to communicate with selected domestic users connected to networks, who use the same traffic exchange node. It is the link with the lowest cost per 1 gigabit, while having the highest bandwidth, and therefore the best quality when reaching users.

Usually, on a peering link, usually, the network used by the end user (client) is available in exactly one intermediate node, which is the traffic exchange node. This results in the lowest latency for domestic and international transit / transmission links. The number of users available through this link is a subset of the domestic transit / transmission link - not all domestic users are available through IX links, but if so, the link to them offers much better quality. Peering links therefore complement the domestic transit / transmission link by significantly reducing the cost and improving the quality of service

of the user's communications with the Organization. Peering links are often, depending on the telecom operator, available for free or for a small fee as an extension to a domestic transit / transmission link. Peering links often use the same physical interface and unused bandwidth of the domestic transit / transmission link. As with the domestic transit / transmission link, the likelihood and effectiveness of a DDoS attack is negligible. In its peering policy, the Organization can define the way of exchanging traffic with the participants of traffic exchange node down to a single AS[7] what allows, in a crisis situation (e.g. DDoS attack flowing from a client/clients of a specific AS), to reconfigure routing, i.e. to switch traffic from this AS to e.g. domestic transit / transmission link or international transit / transmission link (what can vastly reduce the volume of malicious traffic) or, in extreme case, to cut off a given AS. Additionally, as with domestic transit / transmission link, the end users of the link are known to the telecom operator exchanging traffic within the peering node. Governmental services, through cooperation with telecom operators, are always able to reach the end user who generate the traffic (no anonymity / full attribution).
In addition, BGP offers the shortest routes through inter-operator nodes, which significantly reduces the risk of BGP hijacking attacks.
Moving some of the domestic traffic to peering links will not only improve communication with users available through these links, but will also improve communication with other users by reducing the amount of traffic on domestic transit / transmission links and international transit / transmission links.

**d) Resource Links (CDN)**

These types of links are used to communicate with resources that must have high throughput and short / fast response times. This means resources or services that must be located as close as possible to the user and be able to deliver content quickly and with high quality. Examples of such resources are cloud services (e.g., o365, GSuite), social networks, and streaming services that inherently generate a lot of traffic. Resource links support individual, selected services or resources, but with extremely high quality tailored to the characteristics of those services. The use of access links allows for a significant improvement in user experience while taking a significant portion of the traffic off the other links (i.e., international transit / transmission, domestic and peering links). A direct link to the CDN ensures operation of services located there even in the event of a massive DDoS attack on the remaining links used by the organization.

Resource links are available from telecom operators under:

- dedicated VC/VLAN (as is the case with for a peering link) to a traffic exchange node within an existing service, e.g. as another channel of an existing link,
- CDN services usually available in inter-exchange nodes (peering links),
- by directly inserting devices from the service provider (e.g. Google, Youtube, Netflix, Facebook, AKAMAI, CloudFlare, etc.) into the recipient's network. Where the recipient meets requirements/criteria set out by the service provider, the devices inserted into the recipient's network (implicitly the Organization) are free or available at a relatively low cost. This solution takes traffic load off other links, by moving access to the content of the provider's services (e.g., Google) to a cache located in the Organization's network, which greatly improves the quality of the provider's services.

[7] Autonomous System

A resource link has a relatively low cost of data bandwidth per 1 gigabit. On this type of link, resources offered by service providers are directly accessible via a single intermediary node for traffic exchange. As a result, data transmission latency on this link are the lowest of all mentioned links. There is no traffic generated by end users on the resource links, but the use of this link can significantly relieve the load on the other links used by the Organization by transferring traffic generated by the Organization to service providers, e.g., to the Google service. There is no risk of DDoS attack on the CDN link. If the service provider resources are available through such a link this should be THE primary choice of a route to that resource.

### 3. CDN

The optimal method to provide services and content made available by the Organization to end users is through the use of CDN (*Content Delivery Network*) mechanisms. This type of solution works as a cache or proxy located very close (in a network context) to the end customer's infrastructure. telecom operators often use such solutions to improve the quality of access to typical content (e.g. YouTube, Netflix, Google) and to relieve the network backbone and transit / transmission links. It is estimated that 60% of Internet traffic currently terminates in CDNs and is not natively transited to service providers. In practice, the performance of CDNs exceeds the currently available volume of major DDoS attacks many times over, which appears to be sufficient protection against attacks.

CDN services can be delivered in three ways:

1) As a CDN service offered by a large, international provider, CDN services are provided for any content;
2) As a service available from a telecom provider, who delivers any content directly to external users from CDN nodes rather than from servers of the Organization;
3) As a service of large players who insert their cache devices into a network that supports a sufficiently large amount of client traffic. Such solutions are used by Google or Netflix, for example.

The Organization should consider using a CDN as a method to reach end users if the content allows for this type of intermediary. When choosing a CDN as a content delivery method, the Organization must consider the geographic reach of the CDN and the location of its users (it does not make any sense to make services available typically to your national market available through CDN players with global outreach). The organization should also take into account recommendations and legal regulations related to cloud services and their localization in the EU (GDPR regulations or regulations of the National Regulatory Bodies).

### 4. Redundant bandwidth

Having redundant bandwidth for a specific telecom link can often provide adequate protection against minor volumetric attacks. During regular use of a link or ICT infrastructure/system, the total of bandwidth used should not exceed 50% of available resources (understood as the available bandwidth on a given link). In order to protect against this type of attack, it is possible to purchase the 95th (or 98th) percentile bandwidth service from the telecom operator. Such a service provides a much wider bandwidth of traffic than the one contracted with a fee for traffic exceeding a given contract. For example, if the

volume of traffic exceeds the contracted bandwidth, the telecom carrier automatically allocates additional bandwidth to the customer (usually paid in the model of number of gigabits x number of hours of additional bandwidth allocation).

## 5. Link bitrate

An important parameter that ensures quality and availability of services is the bitrate of the link (understood as the number of bits that can be transmitted per time unit) on the side of the provider of a given service, i.e., the Organization. Higher bitrates are obtained by using faster (redundant in relation to the speed of the link on the Organization's side) network interfaces (min. 10 Gbit/s due to the design of this type of interface, i.e., the depth of FIFO queues, the computational power of the chips used to support a given interface) and by multiplying the number of interfaces themselves. This is intended to shorten the time of data packet handling by network devices and to relieve the FIFO queues on these devices. Consideration should be given to the link speeds available at end users, which, due to economies of scale, may be important when generating user connections to the Organization's ICT infrastructure.

Currently, telecom operators provide individual customers with bitrate which, increasingly more often, exceed 1Gbit/s. Therefore, it is necessary to ensure that the Organization's services are provided via links with parameters no worse than those used by customers. This prevents packet queuing on the side of the Organization, and therefore relieves the load on the Organization's equipment and infrastructure, improving both the technological responsiveness of the Organization's services (noticeable to end users) and resistance to overloads and attacks.

It should be remembered that also a telecom operator in its backbone and access network must have redundant bandwidth available, which should ensure proper operation of the operator's network in case of a typical DDoS attack. Prior to link purchase it is worth considering whether the operator really holds such extra bandwidth, both backbone and for connecting the node which terminates the Organization's services.

## 6. Blackholing

When a volumetric DDoS attack occurs, both the ISP and the Organization have the ability to block incoming traffic by directing it to a so-called black hole, i.e., to a non-existent interface (/dev/null).

Blackholing can be implemented in two ways:

a) by writing appropriate rules directing malicious traffic to the blackhole by the service provider (manually or automatically);
b) as a service made available to the client (the Organization) by the telecom operator to be performed independently within the scope of provided telecom links.

Compared to the method based on traffic filtering, this solution is characterized by much lower consumption of router resources and simpler rules management than the use of classic

ACLs. This makes it possible to block unwanted traffic effectively and quickly with minimal consumption of device resources.

Blackholing comes with a risk of blocking the correct addressing, for example, if wrong addresses/classes of addresses are entered, and as a result may impact, e.g.:

a) availability of services provided by the Organization,
b) availability of services by external providers,
c) network stability when blocking of addressing relevant to the operation of the Internet (DNS, RIPE DB, CDN, etc.).

It's important to remember that manual application of blackholing rules will also require manual removal of those rules, e.g. when the attack has stopped.

When choosing an ISP, the Organization should verify whether the provider has blackholing implemented in its network.

## 7. BGP flow specification (flowspec)

Flowspec is an operator-side mechanism which extends the BGP protocol to layer 4 of the OSI model, i.e., in addition to IP address-based routing, it allows for configuration of service-based routing and use of additional flags that allow for routing of traffic along a different route, defined by the administrator. For example, in the case of a DDoS DNS Amplification attack, when using the flowspec mechanism, it is possible to redirect this attack (via port 53) to e.g., a telecom operator's cleaning center service, while maintaining availability of services based on other protocols such as HTTPS.

Unlike blackholing, flowspec allows a telecom operator to filter malicious traffic directed to an IP address of the organization from legitimate traffic, thus preserving the operation of its services.

Flowspec can be implemented in two ways:

c) by entering appropriate rules that direct malicious traffic to flowspec by the service provider (manually or automatically),
d) as a service made available to the client (Organization) by the telecom operator for self-execution within the scope of shared telecom links (it is possible to set up a BGP FS session, where the Organization itself manages the rules forwarded to the telecom operator).

The use of the flowspec mechanism carries the risk of blocking correct services or addressing if wrong addresses/address classes/ports/services were entered, and as a result may affect e.g.:
a) availability of services provided by the Organization,
b) availability of services by external providers used by the Organization,
c) network stability when blocking of addressing relevant to the operation of the Internet (DNS, RIPE DB, CDN, etc.).

When selecting a telecom provider, the Organization should consider the mandatory use of the flowspec mechanism by that provider.

## 8. Cleaning center service

Cleaning center services provided by telecom operators rely on devices in the operator's network which filter malicious traffic from correct traffic. Cleaning center provides much higher effectiveness of filtering unwanted network traffic than blackhole or flowspec solutions.

When an attack is detected, the telecom operator redirects the attack (using for example flowspec or basic BGP) to a dedicated service. Service administrator, using advanced algorithms, filters out unwanted network traffic identified as attack. The rest of the network traffic is directed to the Organization's network.

An important feature of such solutions is off-ramp operation, which means that in a regular situation, production traffic is not directed to such cleaning center at all. This removes latency, shortens packet transition path and minimizes risk of failure (cleaning center failure does not cause basic service to become unavailable). It also greatly increases the capacity of such cleaning center by offloading traffic that does not require filtering.

The telecom operator should ensure high availability of cleaning center services, e.g., through:

a) redundancy,
b) geographical dispersion.

As one of the risks of using cleaning center service we can point to potential false positives, i.e., incorrect filtering of correct production traffic. The use of inline solutions (described below) which work in tandem with telecom operator solutions allows to significantly shorten the time of attack detection and to filter out unwanted network traffic.

## 9. Cloud solutions

Cloud solutions available on the market should be considered an 'cleaning center on demand' where in the case of a DDoS attack, the most optimal route in the BGP path will be the route through the cleaning center of the 3rd party which provides such a service to the Organization.
The main disadvantage of such solution is the fact that all of Organization's traffic, including customers' traffic, can be routed through a geographically very distant node, which completely disrupts local routing policy, significantly worsens service parameters for customers and raises legal issues about processing or analysis of users' traffic by 3rd party located in such communication path.
Such solutions should always be pre-verified for compliance with the recommendations and legal regulations applicable in a given sector. The assessment must especially take into account how the cleaning center analyzes the traffic and whether the data transmitted / transferred is being processed.

## 10. Inline solutions

Apart from services and solutions protecting the Organization from DDoS attacks, which are provided by telecom operators, the Organization should have their own elements of ICT infrastructure to provide protection against DDoS attacks.
This allows for:

a) early detection of attacks of this type and immediate notification of the telecom operator,
b) mitigation of attack (up to capacity of link available to the Organization) by filtering malicious traffic from the genuine one,
c) imposing limits on network traffic up to the capacity of the link available to the Organization, or the capacity of the Organization's infrastructure resources, which allows for protection against DDoS attacks aimed at saturation of infrastructure or application resources,
d) protection against piggy-backing (parasitizing) on the Organization's infrastructure to generate DDoS attacks on other institutions/Organizations (e.g., using DNS Amplification).

Application of inline solution, as the only method of protection against DDoS attacks, cannot be considered an effective mitigation of this type of threats.

It should be noted that the use of inline solutions is the only viable option to repel DDoS attacks targeting application logic without passing encryption keys outside the Organization (traffic is decrypted by the Organization itself).

## 11. Filtering of Network Traffic

Consistent with the principles of minimizing the privileges necessary to provide a given service, the Organization should consider filtering network traffic only for traffic necessary for the operation of the service.

This solution will reduce potential for malicious network traffic to reach devices providing the service that is not related to the service. This applies both to the application layer and the network layer. For example, if the service provided is e.g., HTTPS protocol access, then the remaining network traffic directed to other services of the device (providing HTTPS service) should be filtered (limited / restricted). Similarly, if the service is provided via TCP protocol, the UDP, ICMP etc. traffic directed to this device should be filtered (limited / restricted).

Risk linked to the above solution can include overestimation of capacity of network devices used for traffic filtering, which may cause overloading of the device and failure to deliver its core functionality, thus limiting access to services provided by the organization.

## 12. Control-plane policing

Policies should be implemented to take advantage of available device features, in order to regulate the flow of control traffic for services provided by the device in question. For example, if the Organization's router provides Internet access services via BGP protocol, appropriate filtering and resource limiting / restricting means should be applied according to manufacturer recommendations, so that BGP control messages are processed only from verified neighbors.

### 13. Proper hardware sizing of network devices

DDoS attack angle focused on resource saturation can result in network devices' resource saturation (memory saturation, CPU saturation, FIFO queues, processors on line cards, FPGA processors dedicated to supporting dedicated router functions, parallel connection limits for a given hardware platform, etc.), which can ultimately lead to unavailability of network services.
The organization should ensure proper sizing of network devices used for data transmission. Device parameters should handle traffic that is at least one order of magnitude higher than the Organization's typical production traffic.

### 14. Load balancing and network traffic proxying

The Organization should consider implementing an architecture where the Organization's sites and services are protected by an additional access layer exposed to the client from the Internet. This layer should provide appropriate security rules to inspect client session traffic. The presence of a proxy layer between the Internet and the Organization's front-end layer will help protect the Organization's infrastructure from resource saturation of the application servers.

The proxy layer should also be used for filtering network traffic having regard to the application layer protection by utilizing WAF/DAF-class solutions.

Appropriate configuration of proxy layer parameters (session limits, TLS offloading, one-connect, connection persistence, etc.) will optimize the use of resources on application servers and will reduce the negative effects of attacks that can significantly affect the stability and security of back-end systems.

### 15. Captcha

The Organization should consider implementation of mechanisms against DDoS attacks against the application layer by forcing actual user interaction through solutions such as:

a) Captcha with particular emphasis on UX,
b) mechanisms to restrict traffic auto-generated by the client,
c) detection of bot activity or applications which auto-generate traffic to services provided by the Organization.

This solution also protects against brute force attacks.

When choice of a solution is being made, please remember that free Captcha market solutions may collect users' metadata and redirect users' traffic to the Capcha provider. This means the actual cost of a 'free' solution comes in a form of payment by collection of end user's metadata, which in turn may constitute a breach of law.

### 16. DNS

The Organization should consider implementing technical and organizational solutions to protect against DDoS attacks which aim to undermine DNS service availability that support

the Organization's domains. The operation of the DNS service is essential to the operation of the Organization's services available to external users. When DNS service is taken down, in practice the services offered by the Organization remain as unavailable as with any massive DDoS attack.

The main protection against DNS attacks is implementation of DNS distributed architecture – it is very hard to execute a successful DDoS attack, which will block simultaneously a large number of DNS servers which are geographically dispersed. There are commercial services available, which offer secondary DNS dispersion amongst several hundred locations scattered around the world. This, in practice, appears to be sufficient in terms of technology to secure against DDoS attacks, as well as legal obligations for data processing within the legal remit of the EU.

## III. Procedures

The Organization should have appropriate procedures in place when DDoS attacks occur, including but not limited to:

a) procedures for contacting telecom operators which define rapid escalation paths in the event a DDoS attack is identified,
b) procedures on prioritization of Organization's services which, in a situation of real DDoS attacks will enable management of these services (e.g., restricting / limiting availability of lower priority services while ensuring operation of higher priority ones). In order to optimize and accelerate procedures in this area, the Organization should consider their automation,
c) procedures on crisis communication (including communication with users, media representatives, supervisory body, national authorities, external suppliers, etc.) carried out if a successful DDoS attack, which restricts access to Organization's services attack takes place,
d) procedures which identify key persons required to take actions in the situation of an attack and which help them undertake such actions (e.g., indicate need to work from the Organization's premises if services become unavailable, steps to define the chain of command, etc.),
e) procedures for communication with the relevant CSIRT team (on a sector or domestic level) for immediate notification of an identified attack.

## IV. Testing

The Organization should schedule and perform regular and cyclic tests to validate:

a) infrastructure resilience against DDoS attacks in order to define maximum parameters of this resilience,
b) internal procedures

Each time tests are completed, or in case of a real DDoS attack, the Organization should perform a new risk assessment to re-evaluate, at a minimum:

- need to update procedures,
- requirement to update data communications architecture, including Internet connection architecture,
- update of devices to verify their resources match the threat level.

## V. Security monitoring

Due to widespread availability of CaaS (*cybercrime as a service*), DDoS attacks are a low-cost operation for the attackers.
DDoS attacks can be used to divert attention from other attacks and criminal activities conducted at the same time against other Organization services and sites (i.e., false-flag attack). When a DDoS attack is detected, the Organization should ensure that the security of its infrastructure and services is monitored to a degree that is no lower than that maintained during standard user traffic and fault-free service delivery.

## VI. WAN management via out-of-band (OOBM)

Organization should ensure that it will manage its telecom and IT infrastructure (e.g., WAN management) in case of a DDoS attack, by providing alternative (backup, redundant) links used for administrative purposes, which should be separate from the band used to provide Organization's services.

In telecom networks created within the Organization, in accordance with best practices, a dedicated infrastructure should be created that allows access to management console for at least key components of that infrastructure. As shown by *case studies*[8], full separation from the production infrastructure will ensure uninterrupted access to the device management console in case of extensive failures or ongoing large-scale attacks. Most modern network devices are equipped with dedicated interfaces for their management, and these interfaces come equipped with their own dedicated processors and network chips. This means that even in the event of a widespread DDoS attack that saturates the hardware resources of a network device or server, administrators will still have guaranteed dedicated hardware resources to operate that device console in order to take mitigating actions.

## VII. Separation of corporate traffic from external user services

Separating the traffic dedicated to applications and services provided to external users from the traffic originating from Organization premises, branches, or remote employees, will allow to build a reliable network in which hardware resources and available links will be dedicated to specific tasks. It will also make it possible to ensure appropriate control, filtering and protection mechanisms. These may differ between data center requirements and users located in the Organization's branches, including mobile users of the Organization.
The infrastructure dedicated to application traffic/services provided to external users may have much greater 'power' reserves than the office infrastructure used by the Organization's employees. In particular, the Organization may use the available security and data scrubbing services to adequately mitigate the negative effects of a DDoS attack at the telecom operator level.

Both on-site and remote employees can connect to the Organization's internal systems both via Internet connections and dedicated data transmissions between the Organization's facilities and data centers.
The Organization should consider the availability of a backup VPN hub for key Organization employees to enable them to perform tasks in an emergency situation. The Organization should

[8] Source: https://datacenterfrontier.com/facebook-we-disconnected-our-data-centers-from-the-internet/

also develop emergency procedures in case of unavailability of the VPN connections, including requirement for some employees to be physically present (on premises) in the Organization.
If the Organization relies on services of external providers, it should consider replacing Internet-based communications links with those providers with dedicated connections, e.g., in IP MPLS technology.

## VIII. Automating the execution of emergency scenarios

The Organization should strive to implement automated mechanisms that will work in an emergency situation. These include scenarios that, if an attack is detected that could threaten the continuity of the Organization's operations, would allow for the immediate implementation of predetermined mechanisms to protect and mitigate the effects of the potential attack. Automatic activation of certain processes, such as changing BGP prefix attributes, implementing additional mechanisms to protect hardware resources of network devices and servers (*control-plane policing*), or, in extreme cases, disabling the Internet connection under attack, can significantly contribute towards shortening the response time of the Organization to the attack. In the long run, such an approach will limit the negative effects of an attack and give administrators time to properly attribute and implement detailed dedicated protection mechanisms. However, the realization of this scenario requires the implementation of an out-of-band management infrastructure and the preparation and testing of relevant scenarios and their inclusion in BCPs. It is also important to keep in mind the risks associated with process automation, which in case of incorrect implementation may, in extreme cases, lead to unavailability of the Organization's services.

## IX. Summary

There are no ready, complex solutions, or one universal method of protection against DDoS attacks. Building of attack-resilient infrastructure cannot be understood as merely buying an off-the-shelf product or service, but it should be a systematic approach which aims to design the whole technological chain responsible for provision of the final service, and creates a multilayer protection of the Organization according to the rule of 'defense in depth'.
The actual, resultant resistance of an organization to an attack is the total combination of applied defense solutions and technologies, using the maximum number of those described above to protect the Organization, while taking into account the potential impact of the weakest link.

**TLP color-coding for message recipients**

| | |
|---|---|
| **TLP: RED** | Recipients are allowed to share information / message ONLY with other recipients of this message |
| **TLP: AMBER** | Recipients are allowed to share information / message ONLY within their own Organization, its clients and constituency), only on the need-to-know basis. |
| **TLP: GREEN** | Recipients are allowed to share information / message with their co-workers, within their own and partner organizations and in their circle. They are not allowed to share via public media channels. |
| **TLP: WHITE** | No restrictions on information / message sharing, except for copyright restrictions |