Preparation for Distributed Denial-of-Service (DDoS) Attacks

Cybersecurity Best Practices

B.14

Volume B:
A technical approach

IDB

INCD
Israel National
Cyber Directorate

Originally published by the Israel National Cyber Directorate in Hebrew under the title *Recommendations for Implementation – Best Practices: Preparing against Distributed Denial of Service (DDoS) Attacks.*
© (2020) Israel National Cyber Directorate.

© (2024) Inter-American Development Bank for this translation.

This document was originally published by the Israel National Cyber Directorate (INCD) in Hebrew. Its translation into English was carried out by the cybersecurity team of the Innovation in Citizen Services (IFD/ICS) division of the Inter-American Development Bank (IDB), and it is included as a chapter of the "Cybersecurity Best Practices" collection.

The reader should keep in mind that cybersecurity is a rapidly evolving field. Although these documents reflect established principles, they may be periodically updated as necessary to reflect developments in this field. Additionally, while every effort has been made to present the recommendations and resources in a way that is universally applicable to organizations around the world, the reader may find references that are specific to Israel's cyberecosystem and context (such as the amounts indicated in New Israeli Shekels [NIS], or references to Israeli law or government agencies).

This publication may be downloaded, copied, and distributed, provided that proper attribution is given to the National Cyber Directorate for the original version in Hebrew and to the IDB for the English translation and that the publication is not changed. The opinions expressed in this publication are those of the authors and do not necessarily reflect the point of view of the IDB, its Board of Directors, or the countries it represents.

The original document is available at: **https://www.gov.il/he/pages/ddospr**. Please note that it includes the following disclaimer:

"This document has been prepared by the National Cyber Directorate in order to promote cybersecurity in the Israeli economy. All rights reserved to the State of Israel - National Cyber Directorate. The document has been prepared for the benefit of the public. Duplication of the document or its incorporation in other documents will be subject to the following conditions: the acknowledgment of authorship of the National Cyber Directorate in the format that appears below; the use of the latest version of the document; not making changes to the document. The document contains information of a professional nature, the implementation of which will require knowledge of the systems and adaptation to their characteristics by a professional in the field of cybersecurity. Any comments or references can be sent by email to: tora@cyber.gov.il."

Contents

Foreword

Digital Transformation and the Challenges of Cybersecurity

As digital transformation continues to expand throughout the world, governments, organizations, individuals, and even objects are increasingly connected to the internet. Although digitalization offers undeniable benefits, such as efficient public service delivery, economic growth, and essential connectivity, it also contributes to our growing collective exposure to cybersecurity risks. Recently, the global COVID-19 pandemic has been an important driver of this phenomenon. As a result of widespread social distancing policies, the number of e-commerce transactions and online personal communications grew sharply in a short period of time, along with the number of employees who began teleworking for the first time. In this unprecedented situation, many internet users undertook novel online interactions without enough awareness of the security risks involved. Organizations had to quickly adapt to these challenges by setting up fully remote workflows, often without all of the necessary security measures in place or appropriate guidance to employees.

Cybercriminals are quick to exploit the uncertainty and vulnerability of unsuspecting individuals. Phishing and other social engineering scams proliferated, taking advantage of the global need for information related to the pandemic and the massive use of videoconference applications. In April 2020, Google reported more than 18 million daily malware and phishing emails related to COVID-19 in only a week. Hackers posing as the World Health Organization sent phishing emails and massively spread malicious links to fake videoconference meetings and attachments containing malware. According to the Check Point Research 2021 Security Report, in the first few months of 2020, almost a million attack attempts against Remote Desktop Protocol (RDP) connections, widely used among organizations for employees' remote connections, were observed every day. In fact, RDP attacks were the most popular form of cyberattack, surpassing even phishing emails. In the second half of the year, as more organizations strengthened the security of their remote platforms, hackers focused their efforts on exploiting vulnerabilities in employees' private assets and remote access devices to penetrate their organizations. Although such threats were maximized by this global context, they are not novel and will not go away; we continue to live in an environment of heightened risk, which is particularly serious in regions of the world where cybersecurity policies and technology are less developed and where citizen education and awareness around this issue are lacking. In other words, although the shifts due to the COVID-19 pandemic may revert to what they were before the pandemic, they have brought to light the urgent need to strengthen individual and collective protections against cyberrisks.

Strengthening cybersecurity is essential to safeguard citizens' rights to privacy and property in the digital sphere, promote citizens' trust in digital technologies, and support economic growth through safe digital transformation. In particular, citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services that they need. Moreover, security breaches have a significant negative economic impact. A recent report by McAfee estimated that cybercrime costs the world economy around US$6 trillion annually, or 0.8 percent of global GDP.

Israel: A Global Leader in Cybersecurity

Israel's innovation and entrepreneurship ecosystem is globally recognized as one of the most vibrant in the world, earning it the name Startup Nation. According to the March 2021 OECD Science and Technology Indicators, Israel is the country that invests the highest percentage of its GDP (4.9 percent) in research and development (R&D). The country is host to more than 300 research and development and innovation (R&D&I) centers of multinational companies. Of these, dozens are dedicated to cybersecurity.

It is no surprise that 40 percent of all private investment in cybersecurity worldwide takes place in Israel, which also has one of the world's largest private ecosystems in this area, second only to that of the United States. According to 2021 data, in that year US$8.8 billion were invested in around 131 Israeli companies from this sector, and more than 40 were acquired for a total of US$3.5 billion. Israel has more than 500 cybersecurity startups, and by 2021, 33 percent of the world's "unicorns" were Israeli. Overall, Israel's export of cybersecurity products was estimated in 2020 at US$6.85 billion.

The Israel National Cyber Directorate (INCD) is responsible for securing Israel's national cyberspace and for establishing and advancing its cyberresilience. The INCD operates at the national level to constantly raise the level of security of organizations and citizens, to prevent and manage cyberattacks, and to strengthen cyberemergency response capabilities. Its positioning as part of the Prime Minister's Office clearly demonstrates the centrality and importance of its responsibilities. Its goals include to prepare and enable the Israeli private sector and general public to protect themselves from cyberthreats by adopting cybersecure technologies, publishing best practices, training personnel, and raising awareness. Furthermore, it aims to establish and strengthen the cyberscience and -technology base by developing highly qualified human capital, supporting advanced academic research, engaging in deep technological R&D, and fostering the cyberindustry. The INCD strives to maintain a protected, safe, and open cyberspace for all of the State of Israel's population and businesses and to facilitate the country's growth and its scientific and industrial base.

The State of Cybersecurity in the Latin American and Caribbean Region

The Inter-American Development Bank (IDB) carries out periodic assessments to capture the evolving capacities of its member states to defend themselves against the growing threats in cyberspace. The 2020 Cybersecurity Report, "Risks, Progress, and the Way Forward in Latin America and the Caribbean," developed in partnership with the Organization of American States (OAS), showed that countries were at varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement.

While in 2016, the year of the report's first edition, 80 percent of the countries in the region did not have a national cybersecurity strategy in place, this number had only fallen to 60 percent by 2020. Furthermore, only a few countries manage the exposure of their critical infrastructure, such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors, to cyberattacks. As revealed by the 2020 report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrisome findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

In terms of countries' capacity to manage and respond to cybersecurity incidents, the same study found that 63 percent of countries had security incident response teams in place, such as computer emergency response teams (CERTs) or cybersecurity incident response teams (CSIRTs). However, of the 20 countries that did, only 3 had reached advanced maturity in their ability to coordinate such responses. In fact, 23 out of the 32 countries were still in an initial stage of maturity in this respect. This finding underscored the general need for countries to strengthen the capacity of their teams to effectively coordinate their responses to cyberincidents. Moreover, the report examined the availability of educational and training opportunities in cybersecurity and found that fewer than half of the countries in the region offered formal education in cybersecurity, such as postgraduate, master's, or technical degrees. Needless to say, having sufficient trained professionals is essential to design and implement the cybersecurity policies and measures that are necessary to ensure a country's resilience in the face of increasingly sophisticated and complex cyberattacks.

The Inter-American Development Bank's Support to Strengthen Cybersecurity Capacity in the Region

For the past few years, the IDB has actively supported the region in the development of cybersecurity capacity, the design and implementation of national-level cybersecurity policies, and the strengthening of cybersecurity capabilities in the sectors it helps develop. This support takes a number of forms. The IDB has provided financial assistance amounting to tens of millions of dollars to develop national cybersecurity capabilities through more than 15 public sector investment loan operations, as well as significant additional funding to ensure the cybersecurity of digital transformation investment projects.

It also provides technical guidance and conducts cybersecurity projects across the region through consultancies, assessments, and tailor-made cybersecurity-strengthening projects on topics that include critical infrastructure protection, cybercrime and forensic analysis, design and strengthening of CSIRTs and security operations centers (SOCs), and national and sectoral cybersecurity strategies. In addition, the IDB has made substantial efforts to provide opportunities for Latin American and Caribbean professionals to strengthen and update their skills in this field by regularly offering workshops and training opportunities. These have included two-week cybersecurity executive courses, offered jointly with the Hebrew University of Jerusalem, as well as tailor-made courses on critical infrastructure protection and others targeted for specific sectors. Finally, the IDB has produced several high-impact publications dealing with national and sectoral cybersecurity issues, and continues to update and add to this body of knowledge regularly.[1]

1. See the website of the Data and Digital Government Cluster (DDG) of the IDB's Innovation in Citizen Services (ICS) division: **https://www.iadb.org/en/who-we-are/topics/modernization-state/data-and-digital-government**.

The IDB and the INCD: Joining Forces

The challenges of cybersecurity, like those of the internet itself, are global. Thus, sharing the knowledge and tools to meet these challenges benefits everyone. In recognition of this reality, the INCD and the IDB have partnered to make Israel's expertise in this area accessible to LAC countries. This collaboration has supported the LAC region in the form of executive and technical trainings on advanced cybersecurity topics, cutting-edge conferences for LAC public officials and professionals in the field, and innovative technical assistance projects. This publication is a product of this collaboration. It consists of a series of cybersecurity methodological guides for organizations, developed by the INCD in light of its analysis of risks, attack methods, cyberincidents, and globally accepted standards. These guides have been translated into Spanish and English as a joint activity of both organizations. They are being made available in these languages with the aim of providing access to this body of knowledge to audiences throughout the LAC region and contributing to strengthening cyberresilience in the region.

The challenge of protecting the digital space will continue to grow, along with the need for proven expertise to confront it. The insights contained in these guides are a resource to promote much-needed professional training in cybersecurity in the LAC region. These guides will contribute to raise organizational standards, promote greater awareness and a culture of cybersecurity within organizations and among the general public, and inform decision makers, managers, and leaders in their cybersecurity initiatives. It is our hope that these guidelines will serve as a roadmap for professionals and leaders throughout the LAC region, working together to build a more secure and prosperous future.

Acronyms

Acronym	Definition
API	Application programming interface
BCP	Business continuity plan
BGP	Border gateway protocol
DDoS	Distributed denial of service
DNS	Domain name system
DoS	Denial of service
HTTP	Hypertext transfer protocol
IEEE	Institute of Electrical and Electronics Engineers
INCD	Israel National Cyber Directorate
IOA	Indicator of attack
IOE	Indicator of exposure
IP	Internet protocol
IPS	Intrusion prevention system
ISP	Internet service provider
PCAP	Packet capture
RAdAC	Risk adaptive-based access control
TCP	Transmission control protocol
TTM	Time to mitigation
WAF	Web application firewall

Introduction

General

One of the main threats to systems and infrastructure exposed to the internet is distributed denial-of-service (DDoS) attacks. These attacks disrupt the business activities of organizations that are attacked to the extent of a complete and prolonged shutdown, which causes organizations substantial harm. Following this trend, it can be assumed that the frequency and technical complexity of these attacks will only increase in the future. Therefore, organizations around the globe need to prepare accordingly.

Differences between a Denial-of-Service Attack and a Distributed Denial-of-Service Attack

Denial-of-service (DoS) attack is an inclusive name for a series of attacks that target cyberassets/business processes mainly to disable or disrupt their activity by creating an abnormal load on their resources. In this case, the factor that initiated the attack is a single cyberasset controlled by an attacker. Often, the attacked organization can block the internet protocol (IP) address of the attacking cyberasset, lessening the business impact of the attack.

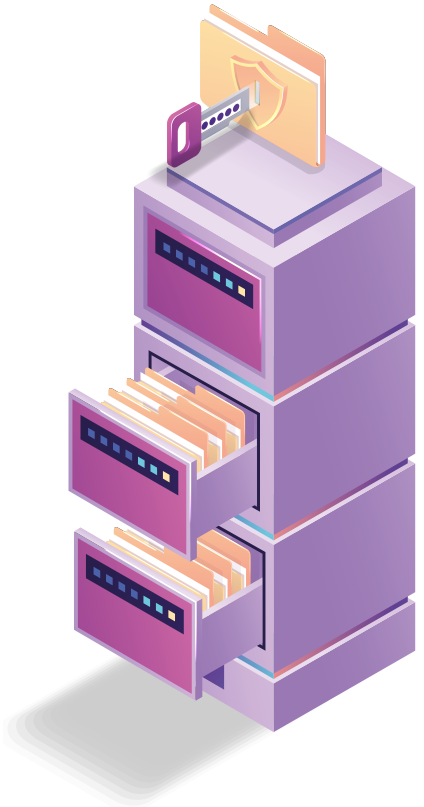
A DDoS attack presents a similar problem, but in this case, the attacker controls a number of cyberassets that work in a coordinated way against the target (such as performing multiple attack waves originating in cyberassets located in different locations around the world). As a result, attack volumes are significantly higher and performing common protective actions, such as blocking the IP addresses of the attacking cyberassets, are not sufficiently effective.

Protection Principles

The protection principles to defend an organization against DDoS attacks are based on the following building blocks: people, processes, and technology.

01

People: The organization is required to ensure that the human capital employed by it and employed by relevant suppliers in the supply chain (such as the internet service provider, or ISP) is able to provide an effective response against conventional cyberattacks, such as DDoS attacks. This includes the involvement of a cybersecurity architect in formulating the solution and examining its effectiveness. The organization should also ensure that it has a cybersecurity incident response team (CSIRT), alongside a 24/7 active monitoring team, so that in the event of a suspected or actual incident, it will be able to detect, identify, and thwart it while minimizing the impact on business activity.



02

Processes: The organization is required to ensure that supportive processes are capable of providing appropriate responses to deal with DDoS attacks. The processes can be divided into the following categories:

- **Power building processes**, which include, among other things, risk management, cyberthreat intelligence (CTI) gathering and analysis, professional trainings, readiness and competency testing (such as resilience testing and exercises), updating attack scenarios and responses in the organization's business continuity plan (BCP), a playbook, and having relevant work practices. In addition, a secure development process[2] is required to address the security design (secure by design) and the security by default while adopting a secure architecture, including ensuring that the infrastructure enables the allocation of resources as needed (auto-scaling) and has the ability to survive and recover from a disaster while minimizing the need for human involvement.
- **Processes for dealing with the attack**, which include, among other things, detecting and identifying the attack and performing protective actions according to the playbook and relevant work procedures.
- **Processes for examining the quality of the response solution currently in place**, while periodically examining the supply of solutions in the market in relation to the needs of the organization.

03

Technology: The organization is required to ensure that the technology protection architecture is adapted to respond to DDoS attacks.

It is common to divide this architecture into three layers of protection, shown in Figure 1.

2. See the document ***The Chief Information Security Officer's (CISO) Guide for Working with Software Development Teams*** soon available within this "Cybersecurity Best Practices" collection.

Figure 1. Protection Layers Architecture against DDoS Attacks

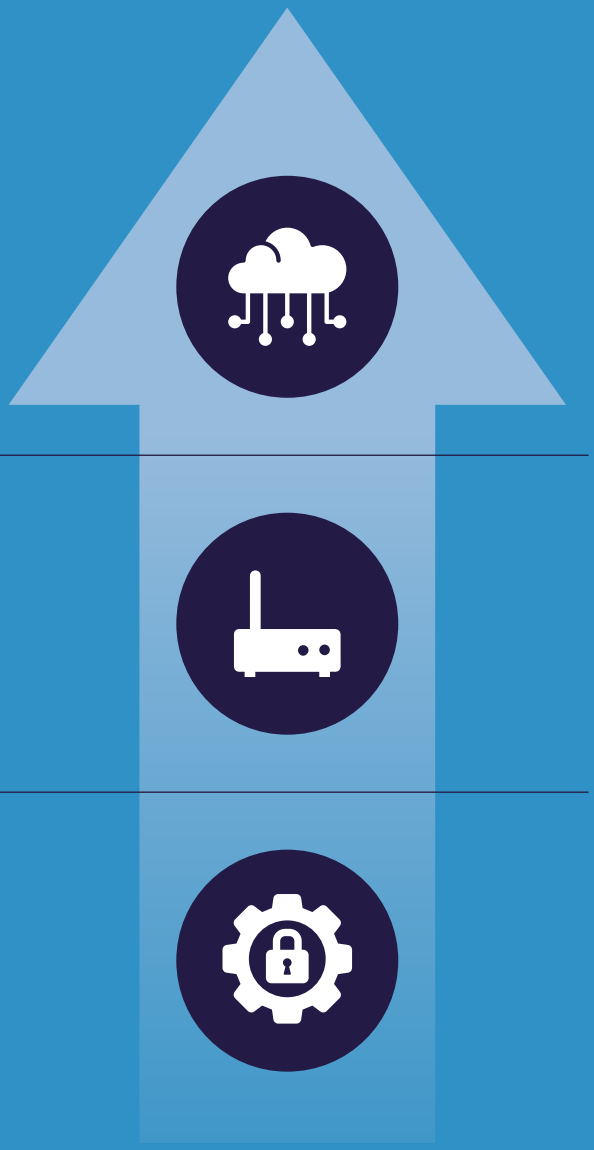


Table 1 provides an overview of each layer of protection according to its role.

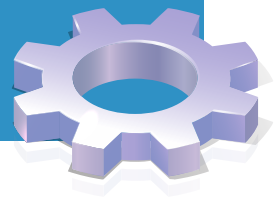
Table 1. Protection Layers against DDoS Attacks

No.	Name of Protection Layer	Role of the Layer
1	Internal layer	Provides direct protection for the cyberassets held by the organization (such as a website). This includes the proper construction of systems and network architecture while implementing common principles, such as secure by design and secure by default.
2	Edge layer	Provides protection for the organization's internet connectivity. It is common for this layer to involve the use of traditional protection solutions and the integration of the ISP's protection capabilities.
3	External layer	Uses third-party entities to decentralize infrastructure and perform advanced protection actions, including the ISP. Nowadays it is common for the actual implementation to be based on purchasing a protection solution in the software-as-a-service (SaaS) model, rather than implementing such a solution independently. It is customary to activate existing security measures in this layer regularly or as needed.

In view of the complexity of protection against DDoS attacks, it is advisable that organizations adopt the defense in depth principle, using it in all layers of protection.

Having layers of protection in practice depends on the architecture and operational environment. For example, when working with a public cloud service provider, the provider may offer their customers built-in protection services, so that the boundaries between the end layer and the external layer may be blurred.

It is important to ensure that the security system complies with new protocols used in cyberspace, such as hypertext transfer protocol version 2 (HTTP/2), HTTP/3, and DNS over HTTP (DoH).



The essential parameter for examining the level of effectiveness of the security arrangement is effective time to mitigation (TTM).

The following is an accepted formula for calculating this parameter:

TTM
=
Time to Detect Attack
+
Time to Apply Effective Mitigation

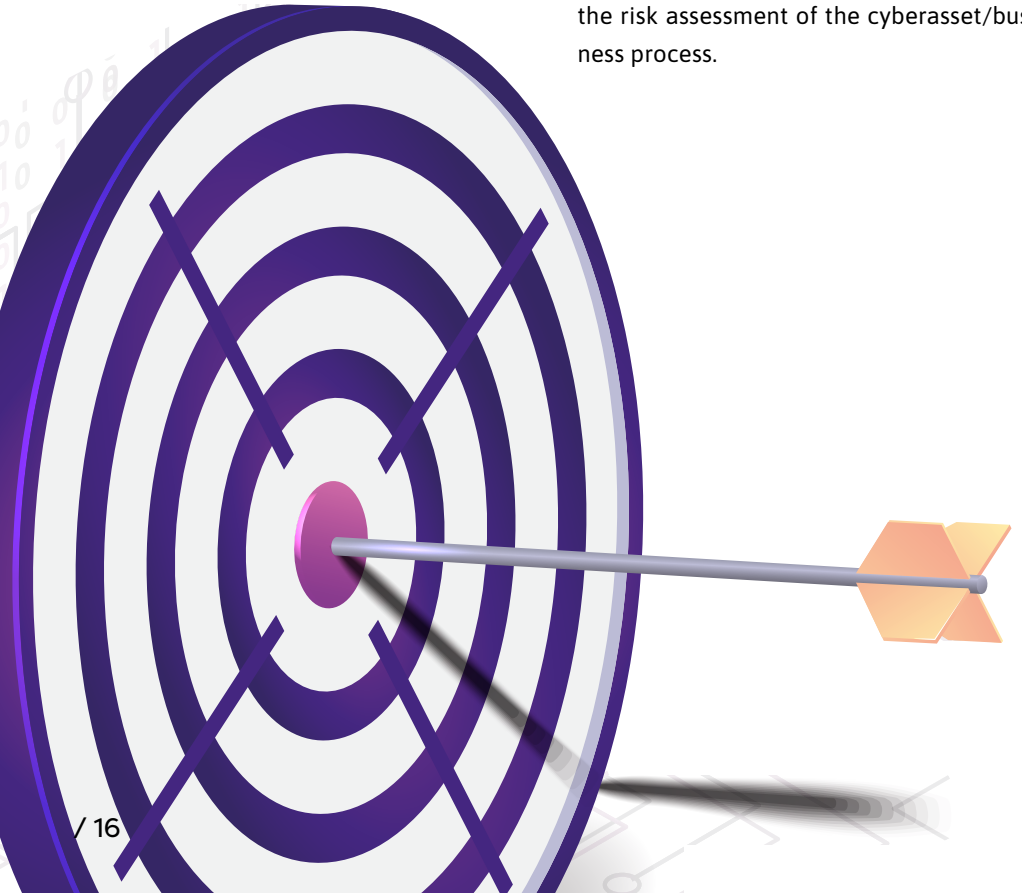
Calculating TTM requires in-depth knowledge of business processes, dependencies, various technical characteristics of the cyberassets, use characteristics of cyberassets (such as the number of active customers at a given time), and performing empirical tests for validation.

Goals and Objectives

The goal of this document is to present best practices for dealing with DDoS attacks.

/01. Target Audience

This document was written for the chief information security officer (CISO), certified cybersecurity methodologies professionals, certified cybersecurity practitioners, cybersecurity technology professionals (cybersecurity architects), and computer network/IT/system professionals. Other audiences that may gain value from this document are the chief information officer (CIO) and business entities required to approve the risk assessment of the cyberasset/business process.



/02. Scope of This Document

This document presents best practices for preparing for DDoS attacks, focused on linking the organization's infrastructure to the internet. It does not expand on subjects on which the Israel National Cyber Directorate (INCD) has written and published dedicated documents. An example of this type of subject is specific protection of systems and infrastructure, which is discussed in ***Cyberdefense Methodology for an Organization 1.0***, written and published by the INCD.[3]

3. The document is available within this "Cybersecurity Best Practices" collection through the following link: **https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/en/Cyber%20Defense%20Methodology%20for%20an%20Oragnization.pdf**.

/03. Threats Derived from a DDoS Attack

This chapter reviews the main threats derived from DDoS attacks.

Table 2. Overview of Major Threats Derived from DDoS Attacks

No.	Threat Name	Description
1	Denial of service (DoS)	An attacker may disrupt business activity to the point of a shutdown for an extended period of time. Effects may be at the level of the individual service/interface (such as an e-commerce site) or a large number of services/interfaces (such as an e-commerce site and a remote employee login interface).
2	Customer abandonment	An attacker who successfully disrupted or disabled the organization's online service business activity could cause customers to abandon it and move to its competitor.
3	Damage to reputation	An attacker who successfully disrupted or disabled the organization's online service business activity may damage the good name of the organization and potential customers may fear joining the organization, which they may perceive to be a less professional or less trustworthy entity.
4	Damage to data reliability and integrity	An attacker could send a burst of sessions to a cyberasset, and after a short time stop the sessions. In the case of cyberassets that use transactions such as database servers, this may compromise data reliability and integrity. Below are several examples: a. Lack of space to write logs on the disk. b. The cyberasset collapses due to the abnormal load. c. Frequently rolling logs that serve the database back and forth may eventually cause their corruption (data corruption), whether due to locks or some other reason.
5	Extortion	An attacker could threaten and carry out a DDoS attack against the organization if a certain condition is not met (such as a monetary payment). If the organization responds to the attacker's demands, there is a high probability for this to invite further acts of extortion.
6	Exploiting the organization's infrastructure to attack a third party	An attacker may exploit the organization's infrastructure to attack a third party. A common example is the use of unprotected internet of things (IoT) devices to implement amplified DoS attacks. In this case, beyond the possible damage to availability, confidentiality, reliability, and integrity of the information and cyberassets involved, this may expose the organization to regulatory sanctions and lawsuits by the parties affected.
7	Reducing the mean time between failures (MTBF)/ Damage to cyberasset reliability	a. Creating an unusual load on cyberassets in an organization can shorten their lifespan and increase the frequency of failures, which can disable or disrupt long-term business processes. b. An increase in expenditure due to failures, which may result in a reduction in the cyberdefense budget.
8	Causing exceptional costs	To maintain expected service levels, organizations may be required to incur exceptional costs due to the need to perform an unusual and unplanned upgrade or activation of the cyberdefense arrangement or cyberassets, increase bandwidth, or increase the capacity of cyberassets. In the case of a public cloud, an attacker may exploit the built-in ability of the cloud infrastructure to increase resources and/or their high availability, and cause exceptional charges for the organization by the cloud provider (economic denial of sustainability, or EDoS).

No.	Threat Name	Description
9	Smokescreen	An attacker could use a DDoS attack as a smokescreen in order to hide the existence of another attack against the organization from its shield.
10	Bypassing a security mechanism by creating an unusual load	An attacker could create an unusual load, which would allow it to exploit a built-in vulnerability in security measures (such as the organization's WAF), and in this manner bypass an existing security mechanism (such as a malicious input filtering mechanism).

Table 3 reviews several common types of DDoS attacks.

Table 3. Overview of Common DDoS Attacks

No.	Category	Type	Examples for Execution	Consequences
1	Volumetric	High bandwidth consumption	Connectionless lightweight directory access protocol (CLDAP), simple service discovery protocol (SSDP), network time protocol (NTP), Memcached	Loss of network connectivity; loss of ability to upload/download
2	TCP state exhaustion	Exhaustion of existing resources	SYN flood, teardrop attack	Slow server response to customer requests or inability to respond to requests at all
3	Application	Overload on application server	HTTP GET flood, DNS flood	Slow response to customer requests by the application or inability to respond to requests at all
4	Application	Overload on app server + Exploitation of existing vulnerability	Slowloris, R-U-Dead-Yet? (R.U.D.Y.), and other HTTP session attacks	Slow response to customer requests by the application or inability to respond to requests at all
5	Application	Overload on business logic management processes	Shopping cart excessive item addition/reduction	Slow response to customer requests by the application, compromised performance, or inability to respond to requests at all

/04. Best Practices: Preparation for a DDoS Attack

This chapter presents a list of recommendations and best practices, which, if properly implemented, will help in preparing against DDoS attacks.

The complete recommendations table in checklist format can be downloaded at this link: **https://www.iadb.org/document.cfm?id=EZIDB0000474-1107652497-62**

Table 4. Best Practices for Preparing against DDoS Attacks

No.	Recommendation
	General Recommendations
1	The organization should define acceptable indices for each business process/cyberasset in accordance with its business needs. It is important to ensure that the indices have been applied to the various cyberassets according to the need. Below are several examples of customary indices: a. Bandwidth: a measure of the amount of data that can be transferred from the source to the destination on a data network over a given period of time. Basic unit of measurement: bits per second (bps). b. Effective bandwidth/throughput: a measure of the actual amount of data passing through a given path, in a limited period of time, considering the following limitations: 1) The size of the information transmitted. 2) Quality of network device performance. 3) The amount of time it takes to transmit the information. Throughput ≤ Bandwidth c. Number of information packets at a given time. Basic unit of measurement: packets per second (pps). d. Number of HTTP/HTTPS requests (or another relevant protocol) at a given time. Basic unit of measurement: requests per second (RPS). e. Delay: the time frame required for a packet to reach from one end to another. Basic unit of measurement: seconds. f. Latency: the time frame required for a packet to reach from one end to another and back. Round-trip time (RTT). Basic unit of measurement: seconds.

No.	Recommendation
	General Recommendations (cont.)
1	g. Jitter: irregular time delay in sending packets on the network. Basic unit of measurement: percent. Sometimes seconds are used as well.[4] h. Packet loss: packet loss is measured as a percentage of the packets lost in relation to packets sent. i. Maximum transmission unit (MTU): the largest information packet that can be transmitted as a single unit on the network, without the need to perform fragmentation. Basic unit of measurement: bytes. j. Number of connections at a given time. Basic unit of measurement: connections per second. k. Lifespan for user activity (session timeout). Basic unit of measurement: seconds. l. Lifespan for transmission control protocol (TCP) keepalive testing. Basic unit of measurement: seconds. m. Effective TTM. Basic unit of measurement: seconds. n. Customary measures from the world of business continuity (e.g., recovery time objective [RTO], recovery point objective [RPO], maximum tolerable downtime [MTD]).
2	The organization should periodically map the range of IPv4/IPv6, fully qualified domain names (FQDNs), and autonomous system number (ASN) addresses in the organization's possession, while considering the logical and physical location of the cyberassets and processes. This includes interviewing the various operating entities and the internet provider, as well as conducting an initiated search in common public databases. Note that cases can be seen in which the organization has equipment (such as heating, ventilation, and air-conditioning [HVAC]) whose damage can result in a cross-cutting shutdown, but the organization is not aware that this equipment is linked to the internet.

4. "Jitter" is defined as the timing changes of signal ends from their original values. The deviation can be in terms of an instance, time, or signal bandwidth; this value is measured in percent.

No.	Recommendation
	General Recommendations (cont.)
3	The organization should conduct a risk assessment to analyze possible effects on business activity in the event of a DDoS attack. Possible implications on activity should be considered together with the organization's suppliers, such as a public cloud provider or an external supplier who maintains the organization's website. Also, relevant threats should be considered with reference to common measures, such as: intensity (250 gigabytes per second [GB/s], 4 terabytes per second [TBps], etc.), type (according to the above), and time (minutes, hours, days, weeks, etc.).
4	The organization should use cyberthreat intelligence to know the latest attack methods and develop a response plan accordingly. This includes following cyberevents that have occurred in organizations worldwide, with an emphasis on organizations in the international and local sector of activity, while examining intensity, type, duration of attack, cyberassets affected by the attack, motive, and identity of the attacker (as far as can be identified with reasonable certainty), frequency of attacks, review of vulnerabilities exploited in the attack, level of effectiveness of the security measures used by the protecting party, derivative consequences (such as downtime/disruption of business activity, whether there was secondary damage such as impact on share value or customer abandonment and transition to competitor, customer and third-party lawsuits), drawing conclusions and best practices to improve readiness and competency for similar events.
	Internal Layer Security Recommendations
5	The organization should ensure that the information and communication technology (ICT) infrastructure and systems are designed in accordance with the secure by design principle. Below are several examples: a. Having a fail-safe practice by using redundancy or an alternative way. It is important to ensure that this practice exists from end to end. b. Having a self-healing mode in case of failure. This can be effectively implemented when using the microservice architecture. c. Switching to stateless work configuration.

No.	Recommendation
	Internal Layer Security Recommendations (cont.)
5	d. Adopting the principles of security chaos engineering. e. Ability to dynamically increase/decrease capacity (auto-scaling). f. Defining thresholds and bars that indicate normal activity and abnormal/suspicious activity, including applying a throttling application programming interface (API). g. Using a content delivery network (CDN) to store static/dynamic content. It is important to ensure distribution to a number of independent sites around the world. h. When working with a public cloud, the provider's recommendations for building the right architecture should be considered. i. Having an effective ability to redirect to working full-time on a public cloud or to redirect to another public cloud service provider or redirect to working at a shadow site of another service provider.
6	The organization should use hardware that supports accepted standards for dealing with loads in data communications. Examples of application are the following standards by the Institute of Electrical and Electronics Engineers (IEEE): a. IEEE 802.1Qbb Priority-Based Flow Control (PFC). b. IEEE 802.3x Flow Control with Pause Frames.
7	The organization should use application load management systems (application delivery controller, or ADC). Make sure that the chosen solution includes the following capabilities: a. Open systems interconnection (OSI) layers 3-7 response. b. Offloading when working with encrypted traffic. c. Offloading when working with TCP content and traffic. d. Checking the liveness of the application by simulating common actions of a typical user. e. Path-based routing: forwarding a client's request to a destination based on a specific uniform resource locator (URL). f. Host-based routing: transferring client's request to a destination based on a specific HTTP header. g. Custom HTTP response to a customer's request.

No.	Recommendation
	Internal Layer Security Recommendations (cont.)
7	h. Field-based routing: forwarding a request to a destination based on standard and custom HTTP headers and methods, query parameters, and source IP addresses. i. Supporting internet content adaptation protocol (ICAP). j. Supporting customary methods for managing a persistence session.
8	The organization should use a WAF and/or runtime application self-protection (RASP). Make sure that the chosen solution includes the following capabilities: a. Built-in anti-bot mechanism. Emphasis should be placed on completing capabilities in HTTP/HTTPS that do not typically exist in intrusion prevention systems (IPSs). b. Built-in anti-fraud mechanism. c. Blocking attacks according to static indicators that are updated several times a day, based on cyberthreat intelligence. d. Support for virtual patches. e. Discovery and detection of threats in an encrypted medium. f. Ability to differentiate between human user activity and machine activity. This includes ensuring support for customary mechanisms to challenge the user. Example of application: Using a completely automated public Turing test to tell computers and humans apart (CAPTCHA), behavioral biometrics, or mathematical puzzles that the client must solve. g. Blocking attacks when an exception from a user's typical behavioral profile is detected. Including a combination of capabilities for anomaly and outlier detection. h. Software development kit (SDK) that enables integration in a mobile application and an ability to examine the state of the technological hygiene of the cyberasset during remote access in real time. i. Masking the identity of cyberassets and system services. For example, replacing default HTTP headers X-AspNet-Version, X-Powered-By values with alternative values. j. Ability to create a new indicator of attack (IOA) without the need for human intervention and without relying on a cyberthreat intelligence service. An example of implementation is the creation of an indicator based on the detection and identification of unique patterns that deviate from an approved baseline or other means.

No.	Recommendation
	Internal Layer Security Recommendations (cont.)
8	k. Providing access according to the risk adaptive–based access control (RAdAC) model. Under this approach, an attribute-based access control (ABAC) model is extended so that user permissions are determined at runtime based on different attributes and considering the level of risk. For example: 1) Integrating cyberthreat intelligence into the security arrangement, including the use of indicators of attack/compromise (IOAs/IOCs) to block attacks and suspicious activity, such as blocking access from a low-trust IP address (low reputation) due to affiliation with a known attack campaign infrastructure or anonymous proxy server. 2) Defining blacklists and whitelists of individual IP addresses and address ranges (source/destination), ports, services, time window, ISPs, geofencing/geolocation,[5] etc. 3) Adoption of customary principles for continuous authentication and adaptive authentication. l. Performing device profiling.
9	The organization should use a customary solution to block the downloading and running of malware in cyberassets to thwart the possibility of recruiting them in favor of carrying out DDoS attacks in real time or in the future.
10	The organization should periodically optimize the content of acceptable files which serve to define which pages search engines should/should not index. Examples of acceptable files: a. robots.txt b. Sitemap

5. Due to the fact that the mapping of IP addresses in relation to geographical location is not always up-to-date/accurate, there may be situations when IP addresses will be used by parties outside your country/region, even though the registry indicates that these addresses are associated with your country/region.

No.	Recommendation
	Edge Layer Security Recommendations
11	The organization should perform a physical/logical separation between the service channels to reduce the effect of the DoS attack on all the various channels (resource management in a separate channel). Below are several examples: a. Separating the remote connection channel (virtual private network, or VPN) from a channel that serves an e-commerce site. b. Separating an internet browsing channel from a business-to-business (B2B) channel. c. Separating an email channel from a channel that serves an e-commerce site. d. Separating an internet browsing channel from a channel that serves voice over internet protocol (VoIP) infrastructure.
12	The organization should use an IPS. Make sure that the chosen solution includes the following capabilities: a. Built-in anti-bot mechanism. b. Blocking impersonations (spoofing). c. Blocking attacks according to static indicators that are updated several times a day, based on cyberthreat intelligence. d. Support for virtual patches. e. Discovery and detection of threats in an encrypted medium. f. Ability to differentiate between human user activity and machine activity. This includes ensuring support for customary mechanisms to challenge the user. g. Blocking attacks when an exception from a user's typical behavioral profile is detected. Including a combination of capabilities for anomaly and outlier detection. h. Blocking typical port scanning activity (e.g., TCP SYN scan, TCP connect scan, UDP port scan, SCTP INIT scan). i. Supporting the ability to transfer suspicious/malicious traffic to a sinkhole and a blackhole. j. Providing access according to the RAdAC model. (See point 8 above.) k. Initiated slowdown of suspicious activity (tarpitting/tarpits). In general, the use of an IPS built into the organizational firewall does not guarantee the same level of durability as when using a dedicated IPS.

No.	Recommendation
	Edge Layer Security Recommendations (cont.)
13	The organization should periodically verify that the access rules in the organizational firewall (ingress/egress filtering) comply with the principle of least privilege access.
14	The organization should periodically verify that an anti-spoofing mechanism is enabled in the firewall and IPS. In this regard, it is recommended to make sure that the organization's assets cannot be connected via the internet using reserved IP addresses. The following is an example of reserved IPv4 addresses: (0/8) loopback (127/8), private (RFC 1918 blocks 10/8, 172.16/12, and 192.168/16), unassigned DHCP clients (169.254.0.0/16), multicast (224.0.0.0/4) and otherwise listed in RFC 5735; and relevant IPv6 addresses.[6]
15	The organization should ensure the application of a rate limit as a means of protecting the various cyberassets (including the communication routers themselves).
16	The organization should use a system for prioritizing inbound/outbound traffic (quality of service, or QoS) in accordance with the needs of the organization.
17	The organization should harden the data communication routers in accordance with the manufacturer's recommendations for dealing with DDoS attacks.
	External Layer Security Recommendations
18	The organization should ensure that a dynamic and immediate increase in bandwidth for the internet can be made. This includes ensuring that the various cyberassets support the required/irregular bandwidth.

6. A list of relevant IPv6 addresses is available at: **https://www.ripe.net/media/documents/ipv6-address-types.pdf**.

No.	Recommendation
	External Layer Security Recommendations (cont.)
19	The organization should use a number of different ISPs, which use independent infrastructure for access outside the country/region.
20	When working with public cloud services, the organization should take the following steps: a. Link the organization to the cloud provider using a communication channel that is not directly accessible to the internet. Example of application: using multiprotocol label switching (MPLS). b. Examining the supply of protection services available with the supplier, while verifying their suitability to the organization's needs. The base packages usually offer a low level of protection, which does not include a response to a DDoS attack that focuses on the application level.
21	The organization should ask the ISP to perform the following actions (clean pipe): a. Providing access according to the RAdAC model. (See point 8 above.) b. Providing access to specific ports/services only (ingress/egress filtering). c. Supporting the ability to transfer suspicious/malicious traffic to a sinkhole and a blackhole. d. Providing the organization with the ability to carry out independent mitigation operations, in accordance with the organizational threat profile. e. Supporting integration with a cloud cleaning solution (scrubbing) of the service provider and/or a third party.[7]
22	The organization should protect the border gateway protocol (BGP) infrastructure.[8]

7. Cloud scrubbing center (CSC).

8. For more information, see the document ***Prevention of and Response to Border Gateway Protocol (BGP) Hijacking*** soon available within this "Cybersecurity Best Practices" collection.

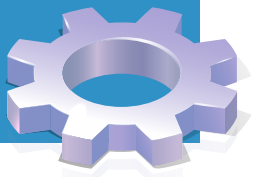
No.	Recommendation
	External Layer Security Recommendations (cont.)
23	The organization should use a scrubbing solution as a compensatory control. In general, it is preferable to use BGP Redirect, rather than DNS Redirect, in light of the fact that the latter leaves the organization's public IP address vulnerable to attacks. It must be determined whether the need for a solution is permanent or whether it can only be activated in the event of a suspicion/cyberincident.
24	The organization should verify that the organization's public DNS infrastructure includes the following capabilities: a. Optimal decentralization at various sites worldwide. b. Global server load balancing (GSLB) and geographic domain name system (GeoDNS) support. c. Built-in protection against DDoS attacks.
	Continuous Monitoring
25	The organization should use a user experience examining system when accessing from the internet to detect and identify features that may indicate a DDoS attack. Example of application: using the application performance management (APM) system.
26	The organization should perform continuous monitoring of the BGP topology affecting the organization's infrastructure.
27	The organization should collect and analyze artifacts from the three layers: a. Internal layer b. Edge layer c. External layer Note that in order to collect information from the external layer, the organization may be required to query the APIs of the relevant parties.
28	The organization should monitor the recommended indicators (see Appendix 1).
29	The organization should collect telemetry from the various cyberassets to discover and optimally identify the tactics, techniques, and procedures (TTPs). Make sure that the solution used has the ability to generate visibility from end to end while maintaining application state-awareness.

No.	Recommendation
Continuous Monitoring (cont.)	
30	When working with a public cloud, the organization should collect data about real-time cost center changes by querying the service provider's API.
31	The organization should conduct a periodic examination from the internet to detect and identify indicators of exposure (IOEs) that could potentially be exploited to increase the effectiveness of a DoS attack, and to take corrective actions accordingly. For the detection and identification of IOEs, security rating services (SRS) or a different solution should be used.
Readiness for a Cyberincident	
32	The organization should update the BCP on relevant scenarios and should ensure that it has an orderly working procedure of incidents/responses.
33	The organization should ensure that it has an acceptable packet capture (PCAP) method to capture network traffic that reaches the organization's gates. Example of application: using a terminal access point (TAP) or network packet broker (NPB).
34	The organization should perform periodic exercises to examine the level of competence and readiness of the organization and any overlapping entities (such as the ISP). Below are examples of scenarios to examine: a. Increasing bandwidth immediately. b. Performing a stress test to examine the level of resilience of cyberassets. c. Performing a tabletop exercise to practice the implementation of the response procedure to a DDoS attack by the relevant parties in the organization. d. Initiating a blockade of a potential attacker at the organization level, at the ISP level (according to the access control list [ACL]), and at the level of the cloud cleansing station (scrubbing center) provider. e. Redirecting work to an alternative location (disaster recovery [DR] site). f. Initiating transition to work with a cloud cleansing station (scrubbing center) and back. Appendix 2 contains recommendations for a playbook for responding to a DDoS attack.[9]

9. For more information, see the document ***Cyberpractice: Creating and Conducting Cybersecurity Exercises for the Organization***, available within this "Cybersecurity Best Practices" collection through the following link: **https://publications.iadb.org/en/cyberpractice-creating-and-conducting-cybersecurity-exercises-organization-cybersecurity-best**.

No.	Recommendation
Supply Chain	
35	The organization should legally anchor the above security requirements with the relevant service providers. It should ensure that acceptable standards are applied in the collaboration agreement, such as: a. Time required to detect and identify an attack (time to detect attack). b. Effective TTM. c. Time to perform effective mitigation. d. Time required to send an alert (time to alert) to the relevant parties. e. Time required to divert traffic to the cleansing service provider (time to initiate diversion). f. Ratio between past malicious traffic and blocked malicious traffic (consistency of mitigation). g. Protection services availability.
36	The organization should legally ensure that protection solution providers are required to present the organization with a new IOA in accordance with the time limit set forth in the service-level agreement (SLA). This includes making sure that there is a regulated process in which the organization presents the solution provider with a PCAP of the attack, and the provider generates an IOA accordingly.
37	The organization should ensure that the relevant service providers comply with the supply chain method of the INCD.[10]

When working with third-party security measures, ensure their operation will be continuous (always-on) or that they will act only in case of suspicion of a cyberincident (on-demand). The organization should formulate the appropriate implementation strategy, in light of the derived consequences.



10. The document ***Supply Chain*** is available within this "Cybersecurity Best Practices" collection through the following link: **https://www.gov.il/BlobFolder/generalpage/expsupplychain/en/Supply%20chain.pdf**

Appendices

Appendix 1. Recommended Indicators for Monitoring

This appendix presents a list of sample indicators that are recommended for monitoring in real time.

Table A1.1. Indicators for Preparing against DDoS Attacks

No.	Indicator
Data Communication	
1	Abnormal increase in bandwidth consumption from/to the internet (at the level of a specific cyberasset, accumulated cyberassets, or all cyberassets).
2	Repeated access using exceptional communication ports, such as internet control message protocol (ICMP).
3	An abnormal increase in the number of times the TCP handshake process is not properly completed.
4	An abnormal increase in the number of disconnections shortly after the completion of the TCP handshake process.
5	An abnormal increase in the number of incidents of packet loss.
Data Communication (cont.)	
6	Initiating independent access to the internet by cyberassets located in the inner layer and/or the edge layer.
7	Repeated port scanning.
8	Inconsistency between the communication port number and the type of application that uses it (mismatched port-application traffic). Example of application: access to the website using port TCP 80, when the traffic content is a file transfer protocol (FTP) application.
9	Repeated use of an HTTP method that is not acceptable on the site.
10	Anomaly in the frequency of delivery of information packets of unusual size within a defined time frame.
11	HTTP query/response size anomaly within a defined time frame.
12	DNS query/response size anomaly within a defined time frame.
13	Anomaly in the number of user requests (DNS/HTTP, etc.) within a defined time frame.
14	Access from low-trust IP addresses (low reputation), such as an IP address associated with an anonymous proxy server, association with a known attack campaign, etc.
15	Re-transmission of an old message (replay-attack).
16	Unusual number of links from a single IP address.
17	Unusual number of packets with time to live (TTL) = 0.

No.	Indicator
Cyberassets: Application and Session Management	
18	Abnormal increase in resource consumption of a specific cyberasset, accumulated cyberassets, or all cyberassets. Examples of application: a. Unusual increase in the number of reading/writing actions to the disk and/or database. b. Unusual increase in the number of times log rollbacks are performed on a database server. c. Unusual increase in disk space consumption. d. Unusual increase in random-access memory (RAM) consumption. e. Unusual increase in the number of links. f. Unusual increase in TCP connection time. g. Unusual increase in the number of information packets. h. Unusual increase in the number of HTTP/HTTPS requests or another relevant protocol.
19	Unusual increase in the number of additions to the user's shopping cart on the site of items with limited inventory without intending to complete the purchase, thus preventing other customers from purchasing the item because it currently appears out of stock (cart/inventory hoarding).
20	Unusual increase in the number of mistakes in entering gift card details (gift card cracking).
21	Unusual increase in the number of additions/removals of items in the user's shopping cart on the site.
22	An anomaly in the average session time of users.
23	Repeated requests from a legitimate user account to the organization's cyberassets from different geographical locations within a short time frame (geo-velocity).

No.	Indicator
Cyberassets: Application and Session Management (cont.)	
24	Access from a cyberasset that uses an unacceptable user-agent.
25	Access from a cyberasset that uses a user agent of an acceptable search engine, but the IP address is not associated according to the manufacturer's publications for the search engine. This can be done by reverse lookup or in other ways.
26	Access from a cyberasset whose browser does not provide the same functionality as the official version of the manufacturer. Example of application: checking that the document object model (DOM) tree on the browser side is intact.
27	An unusual increase in the number of successful/unsuccessful verifications within a given time frame.
28	Increased frequency in the null referrers web server blogs.
29	Increased frequency of sending unusual HTTP status codes to user requests, with an emphasis on: a. Redirects (300–399) b. Client errors (400–499) c. Server errors (500–599)
30	Unplanned collapse or boot of a cyberasset/system services.
31	Increase in average response time to new/existing customer requests.
32	Unusual financial expenses for public cloud services use.

Appendix 2. Highlights for a Playbook for Response during a DDoS Attack

This appendix presents recommendations for a playbook to respond to a DDoS attack.

Table A2.1. Playbook for Response during a DDoS Attack

No.	Action to Be Performed
Intra-Organizational Activities	
1	The organization should alert decision makers (business entities, crisis management team, spokespersons, etc.) about the attack, with reference to common issues, such as: a. Cyberassets and business processes that are or may be affected by the attack. b. The intensity of the attack and the derivative business consequences/ direct and indirect damage control (such as abandonment of X customers per minute or financial loss of Y amount of money). c. The time at which the attack is expected to affect the organization (as far as can be predicted based on previous events worldwide). d. Target audience (internal/external customers, suppliers, etc.) of the attack. e. The standard in which the organization's security measures were not effective enough, in relation to a given point in time.
Intra-Organizational Activities (cont.)	
2	The organization should increase the level of alertness of internal parties, such as alternative service channels (for example, a call center that may need to deal with an exceptional call volume resulting from legitimate customer inquiries or initiated inquiries by an attacker whose purpose is to impair the availability of the telephone service channel simultaneously with online service channels), information systems, and the cyberprotection team (with an emphasis on the cybermonitoring team).
3	The organization should perform tests to detect involuntary changes and anomalies in cyberassets, which may indicate that the DDoS attack is a smokescreen for the real attack.
4	The organization should publish an update about the attack to the users of the organization and indicate the expected behavior on their part.
5	The organization should increase the capacity of the technological infrastructure to compensate for the damage to the level of service created by the attack. Examples include: a. Adding additional web servers. b. Increasing internet bandwidth. c. Redirecting to working in a public cloud.
6	The organization should ensure the operation of the existing security measures at its disposal, including by initiating the transition (as needed) to work with a cloud cleansing station (scrubbing center). In addition, it should carry out continuous monitoring of the effectiveness of the security measures.
7	The organization should record the traffic through the use of PCAP to enable the creation of a new dedicated IOA.

No.	Action to Be Performed
Intra-Organizational Activities (cont.)	
8	The organization should examine the possibility of performing containment actions such as: a. Redirecting to working in a public cloud/shadow site. b. Disconnecting non-essential cyberassets from the internet. c. Stopping systems and infrastructure upgrade processes.
Actions Involving External Entities	
9	The organization should consider issuing an alert to affected target audiences. For example: a. Posting a warning on the organization's website about possible slowness when accessing services, and redirecting them to alternative service channels. b. Updating relevant regulators. c. Updating external support entities. d. Alerting substantial suppliers in the supply chain axis.
10	The organization should update the cyberthreat intelligence provider about the attack.
11	The organization should update the INCD about the attack. The local number in Israel of the call center is 119.
Actions Involving the Internet Service Provider	
12	The organization should contact the ISP and update them about the attack, while jointly implementing acceptable protection controls at the provider level, such as blocking the range of IP addresses used by the attacker.
13	The organization should ask the ISP to contact its sub-providers to block the attack at the source provider level and to take action to remove the attacker's grip from the network.

No.	Action to Be Performed
Actions at the End of the Event	
14	The organization should perform a direct and indirect damage control process (including performing recovery actions, if necessary, and examining possible impact on share value).
15	The organization should conduct threat hunting to detect and identify a grip that the attacker may have left but whose existence current security systems are unable to detect and identify.
16	The organization should update the internal/external factors regarding the end of the event.
17	The organization should examine the effectiveness of the security arrangement (including the relevant service providers) in relation to the indices that were originally approved by management. Below are some examples of customary indices: a. Time required to detect and identify an attack (time to detect attack). b. Effective TTM. c. Time required to perform effective mitigation (time to apply effective mitigation). d. Time required to send an alert (time to alert) to the relevant parties. e. Time required to divert traffic to the cleansing service provider (time to initiate diversion). f. Ratio of past malicious traffic to blocked malicious traffic (consistency of mitigation). g. Availability of protection services.
18	The organization should draw conclusions and lessons learned to improve its ability to respond to future events.

Appendix 3. About the Elaboration of This Document

This appendix explains how this document was developed and feedback conveyed on the content, specifically regarding the need for transparency and proper disclosure of the process and the factors involved.

Formulation of the Document: Market Survey/Syllabus/ Worldwide Comparison

01

Documents and standards from around the world were collected and analyzed from the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and other organizations (main examples are presented in the Bibliography that follows this appendix).

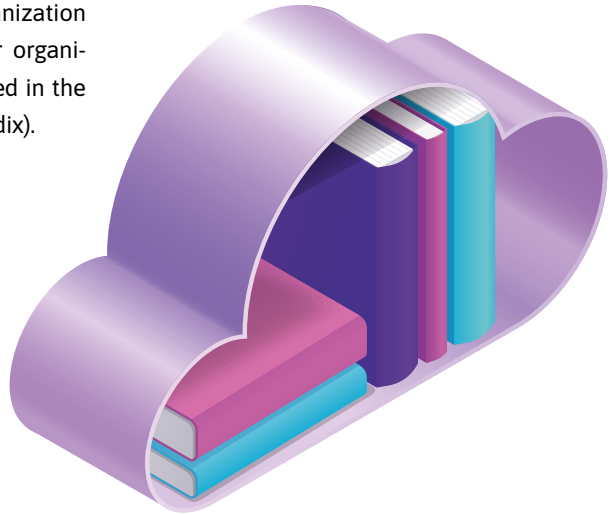
02

Acceptable publications in the field were examined (main examples are presented in the ***Bibliography*** that follows this appendix).

03

The following provided feedback on the draft documents that were published:

- Allot Ltd.
- F5, Inc.
- Imperva, Inc.
- Radware Ltd.
- Mr. Daniel Ehrenreich



Bibliography

Sources of Information in Hebrew

Israel National Cyber Directorate

- Denial-of-Service (DDoS) Attacks: Possible Technological Solutions. Available at: **https://www.gov.il/he/pages/ddos_solutions**.

General

- Denial-of-Service Attack, and how has the East Coast Internet been disabled? Available at: **https://web.archive.org/web/20230328181756/https://softwarearchiblog.com/2016/10/%D7%94%D7%AA%D7%A7%D7%A4%D7%AA-%D7%9E%D7%A0%D7%99%D7%A2%D7%AA-%D7%A9%D7%99%D7%A8%D7%95%D7%AA-%D7%95%D7%9B%D7%99%D7%A6%D7%93-%D7%94%D7%90%D7%99%D7%A0%D7%98%D7%A8%D7%A0%D7%98-%D7%91%D7%97%D7%95%D7%A3.html**.

Digital Whisper

- Increased DoS Attacks. Available at: **https://www.digitalwhisper.co.il/files/Zines/0x4B/DW75-4-AmplifiedDDoS.pdf**.

- Potential for DDoS Attacks in the Israeli Internet Space. Available at: **https://www.digitalwhisper.co.il/files/Zines/0x36/DW54-3-DDoS.pdf**.

Sources of Information in English

Israel National Cyber Directorate (included in this "Cybersecurity Best Practices" collection)

- Advanced Multi-Factor Authentication against Cybersecurity Threats (available soon).
- The Chief Information Security Officer's (CISO) Guide for Working with Software Development Teams (available soon).
- Cyberdefense Methodology for an Organization 1.0. Available at: **https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/en/Cyber%20Defense%20Methodology%20for%20an%20Oragnization.pdf**.
- Cyberpractice: Creating and Conducting Cybersecurity Exercises for the Organization. Available at: **https://publications.iadb.org/en/cyberpractice-creating-and-conducting-cybersecurity-exercises-organization-cybersecurity-best**.
- Organizational Preparedness for a Cybercrisis: Characterization and Requirements of Crisis Management Teams and Incident Response Teams. Available at: **https://www.gov.il/BlobFolder/news/cybercrisisforir/en/Cyber%20crisis_575941_eng%20final%2028.11.pdf**.
- Prevention of and Response to Border Gateway Protocol (BGP) Hijacking (available soon).
- Suppliers' Questionnaire to Strengthen the Supply Chain. Available at: **https://www.gov.il/BlobFolder/generalpage/expsupplychain/en/Suppliers%20Questionnaire%20v1.3.xlsx**.
- Use of Cloud Services: Addendum to the Cyberdefense Methodology for an Organization. Available at: **https://www.gov.il/BlobFolder/policy/cloud_services/en/Use%20of%20Cloud%20Services%20En.pdf**.

General

- AWS Said It Mitigated a 2.3 Tbps DDoS Attack, the Largest Ever. Available at: **https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/**.
- Exponential Growth in DDoS Attack Volumes. Available at: **https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks**.
- Guide to DDoS Attacks. Available at: **https://www.cisecurity.org/wp-content/uploads/2017/03/Guide-to-DDoS-Attacks-November-2017.pdf**.
- How to Fake Spoof Your Location Google Chrome. Available at: **http://web.archive.org/web/20220117083702/https://dowpie.com/fake-spoof-geo-location-google-chrome/**.
- HTTP Response Status Codes. Available at: **https://developer.mozilla.org/en-US/docs/Web/HTTP/Status**.
- IPv6 Address Types. Available at: **https://www.ripe.net/media/documents/ipv6-address-types.pdf**.
- Mitigating IoT-Based DDoS. Available at: **https://www.nccoe.nist.gov/sites/default/files/legacy-files/iot-ddos-project-description-final.pdf**.
- Network Denial of Service. Available at: **https://attack.mitre.org/techniques/T1498/**.
- Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing. Available at: **https://www.rfc-editor.org/info/bcp38**.
- OWASP Automated Threat Handbook. Available at: **https://github.com/OWASP/www-project-automated-threats-to-web-applications/tree/master/assets/files/EN**.
- Re-Hash: The Largest DDoS Attacks in History. Available at: **https://www.thesslstore.com/blog/largest-ddos-attack-in-history/**.

- The Top 10 DDoS Attack Trends. Available at: **https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf**.
- Top 15 Indicators of Compromise. Available at: **https://www.darkreading.com/cyberattacks-data-breaches/top-15-indicators-of-compromise**.
- Understanding Denial-of-Service Attacks, Security Tip (ST04-015). Available at: **https://www.cisa.gov/news-events/news/understanding-denial-service-attacks**.
- Worldwide DDoS Regulations. Available at: **https://government.cioreview.com/cxoinsight/worldwide-ddos-regulations-nid-146-cid-30.html**.

Allot

- DDoS Attack Handbook. Available at: **https://www.allot.com/resources/Enterprise/HBK-DDoS-Attack-Handbook-for-Enterprise-May-2021.pdf**.
- Service Provider Requirements for DDoS Mitigation: Protecting and Optimizing Networks for Modern Threats and Future Scale. Available at: **https://www.allot.com/resources/WP-Frost_Sullivan-DDoS-Mitigation-Requirements.pdf**.

Akamai

- Making a DDoS Protection Plan: 8 Best Practices. Available at: **https://www.akamai.com/site/en/documents/white-paper/akamai-8-steps-to-a-ddos-mitigation-plan-white-paper.pdf**.
- Mitigating DDoS Attacks in Zero Seconds with Proactive Mitigation Controls. Available at: **https://www.akamai.com/site/ja/documents/white-paper/proactive-ddos-mitigation-with-prolexic-mitigation-controls-whitepaper.pdf**.

F5

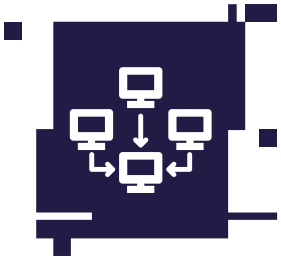
- Blocking Bots: How Silverline Shape Defense Works. Available at: **https://community.f5.com/kb/technicalarticles/blocking-bots-how-silverline-shape-defense-works/279595**.
- Defeat Bot Attacks with New Silverline Shape Defense Managed Service. Available at: **https://www.f5.com/company/events/webinars/defeat-bot-attacks-with-new-silverline-shape-defense-managed-service**.
- Mitigating Application DDoS Attacks. Available at: **https://www.f5.com/c/emea-2020/event/f5-myforum/myforum-mitigating-app-ddos-attacks**.

Radware

- DDoS Survival Handbook. Available at: **https://www.radware.com/getattachment/8c94ccc1-5a50-450a-b4f1-061af8193118/294edae9-d1e3-4342-ad6e-e36cd037aeb3.pdf.aspx**.
- How To Protect Yourself Before, During and After a DDoS Attack. Available at: **https://www.radware.com/getattachment/7f2d83d8-bd3f-4201-9e8e-1a5dce0988db/How-To-Protect-Yourself-Before-During-And-After-DDoS-Attack_2022_Guide.pdf.aspx**.
- A Snapshot of DDoS Regulations: 6 Protection Initiatives. Available at: **https://blog.radware.com/security/2014/05/snapshot-ddos-regulations/.**

Gartner

- DDoS: A Comparison of Defense Approaches. Available at: **https://www.gartner.com/en/documents/3907156**.
- Solution Comparison for DDoS Cloud Scrubbing Centers. Available at: **https://www.gartner.com/en/documents/3983636**.



One of the main threats to systems and infrastructure exposed to the internet is denial-of-service (DoS) attacks, a series of attacks that target cyberassets/business processes mainly to disable or disrupt their activity by creating an abnormal load on their resources. A distributed denial-of-service (DDoS) attack presents a similar problem, but in this case the attacker controls a number of cyberassets that work in a coordinated way against the target. As a result, attack volumes are significantly higher and common protective actions are not sufficiently effective.

These attacks disrupt the business activities of organizations that are attacked to the extent of a complete and prolonged shutdown, which causes organizations substantial harm. Following this trend, it can be assumed that the frequency and technical complexity of these attacks will only increase in the future.

This guide presents best practices for preparing for DDoS attacks, focused on linking the organization's infrastructure to the internet. The document was written for the chief information security officer (CISO), certified cybersecurity methodologies professionals, certified cybersecurity practitioners, cybersecurity technology professionals (cybersecurity architects), and computer network/IT/system professionals. Other audiences that may gain value from this document are the chief information officer (CIO) and business entities required to approve the risk assessment of the cyberasset/business process.

Cyberspace is a field of opportunities in terms of technological progress, connectivity, integration, and global connection to the internet. But it is also a field of threats and risks. Cyberattacks can harm organizations and inflict significant financial and image damage. To be prepared to defend against cyberthreats, an organization must master a large number of specializations, whether they are technological, organizational, or process centered. The list of documents presented below reflects the state of the collection at the time of publication of this document.

Volume A: A methodological approach

Volume B: A technical approach

- **B.01** Securing Internet of Medical Things (IoMT) Components
- **B.02** Securing Access Point Name (APN) Infrastructure
- **B.03** Hardening Computer Systems
- **B.04** Reducing Cybersecurity Risks in Video Surveillance Cameras
- **B.05** Reducing Cybersecurity Risks at the Organization's Endpoints
- **B.06** Securing Enterprise Resource Planning (ERP) Systems
- **B.07** Preparation for and Response to a Ransomware Attack in the Organization
- **B.08** Reducing Cybersecurity Risks for Industrial Control Systems (ICS)
- **B.09** Cybersecurity Risk Survey Template for Industrial Control Systems (ICS)
- **B.10** Securing Voice over Internet Protocol (VoIP) Infrastructure
- **B.11** Advanced Multi-Factor Authentication against Cybersecurity Threats
- **B.12** Major Cybersecurity Threats of Remote User Support Platforms
- **B.13** Prevention of and Response to Border Gateway Protocol (BGP) Hijacking
- **B.14** Preparation for Distributed Denial-of-Service (DDoS) Attacks
- **B.15** Reducing Cybersecurity Risks in Building Management Systems (BMS)
- **B.16** Cybersecurity through Mobile Device Management (MDM/EMM) Systems
- **B.17** Securing Managed File Transfer (MFT)
- **B.18** Cybersecurity Aspects of Commercial Message Distribution (SMS)
- **B.19** The Israeli Cyber Emergency Response Team (CERT) Principles of Operation
- **B.20** Securing Multimedia Systems
- **B.21** Integrating Principles of Cybersecurity in the Backup and Recovery Processes

Volume C: Secure software development