Reducing Cybersecurity Risks at the Organization's Endpoints

Cybersecurity Best Practices

B.05

Volume B:
A technical approach

IDB

INCD
Israel National
Cyber Directorate

Originally published by the Israel National Cyber Directorate in Hebrew under the title *Defense Recommendations: Reducing Cyberrisks at Endpoints in the Organization.* © (2018) Israel National Cyber Directorate.

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).

The original document is available at: **https://www.gov.il/he/pages/endstation**. 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]

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.

[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**.

Purpose of This Document

The purpose of this document is to recommend measures that allow the protection of endpoints by creating the following security circuits: physical security and access prevention, permissions, information protection, and security software.

The document recommendations can be implemented in fixed stations within the organization, in mobile stations, and when connecting endpoints that are not the property of the organization to the intranet (such as when there is a bring your own device [BYOD] policy in place).

The document generally refers to an endpoint regardless of the operating system. However, most of the examples and screenshots were taken from Windows, which is the most common operating system for endpoints.[2]

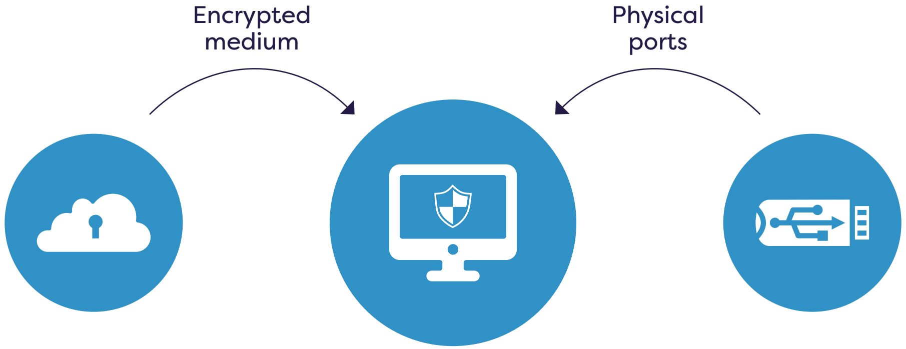
[2] Windows hardening rules can be accessed at: **https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines**. Hardening rules for a Linux station can be accessed at: **https://www.networkworld.com/article/957793/linux-hardening-a-15-step-checklist-for-a-secure-linux-server.html**.

Target Audience

This document is intended for company executives, IT managers, and information security managers who want to improve the level of information security in their organization by improving the level of security at endpoints. Due to the technical nature of some of the recommendations, they must be implemented by professionals with relevant training and experience.

The Threat

Graph 1. Access mapping and attack opportunities



The endpoint is an attractive target for attackers and can serve as a bridgehead for attacking the organization. In this document, we will consider personal computers to be the endpoint of the employee in the organization.

The organization's endpoints can be attacked in a variety of attack vectors and for a number of purposes:

- By inserting a physical memory device, such as a portable drive that contains a harmful file.
- By linking the endpoint to an external network, such as the internet.
- By stealing the endpoint, especially if it is portable.
- Through unauthorized access to a endpoint, physical hacking, or combining hardware or software. Examples include inserting a keylogger eavesdropper or inserting a trojan horse into the endpoint for the purpose of stealing the information on it or to hop to other computers in the organization, etc.

/01. Physical Security and Denial of Access

The Hardening Principle

The hardening principle is prevention of unauthorized access and physical security: basic security measures that must be implemented to secure the endpoint. Its purpose is to prevent the loss or theft of hardware, which can cause incalculable damage to the organization. Therefore, physical security mechanisms must be applied to endpoints.

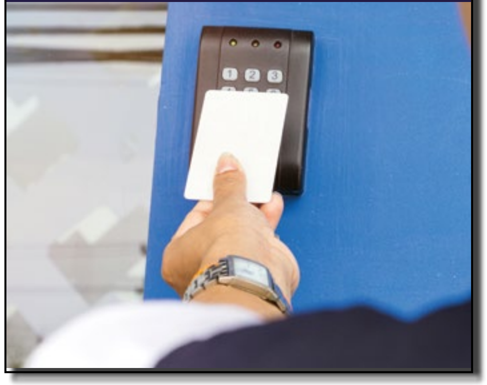
The Hardening Process

Physical security of the endpoint will be carried out in several layers:

01

At the area level, ensure that the work area is protected and only authorized persons have access to it. For example, implement an access control system based on proximity tags.

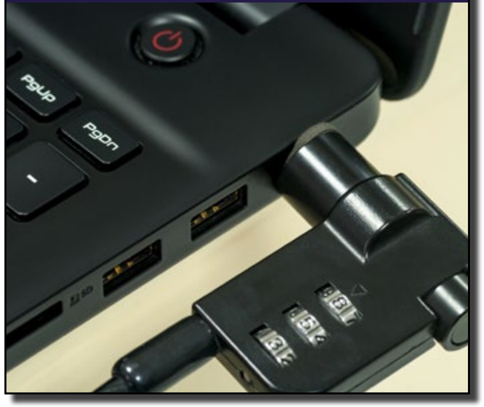
Figure 1. Access control system based on proximity tags



02

At the endpoint level, use a security cage or a security cable lock as a large-scale and permanent means to secure all workstations. This prevents the possibility of detachment and theft of the endpoint from its location.

Figure 2. Security cable lock for endpoints



03

Implement an automatic mechanism for locking the endpoint after a specified period of nonuse.

04

Employees must sign and commit to using the appropriate procedures for protecting and maintaining the endpoint (such as locking the workstation with a password, preventing access to the work area, etc.).

Note! The organization must have a physical security policy in place.

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 > Group: **Physical and Environmental Protection** > 18.1

/02. Access and Permissions

Secure Boot

01

The Hardening Principle: Secure Boot is a feature implemented in PCs that loads the operating system signed and certified. This prevents rootkit-type malware from operating and controlling the endpoint. Ensure that the organization will only use operating systems that support Secure Boot.

02

The Hardening Process: Usually, when operating systems are installed, the Secure Boot feature is enabled by default. To prevent rootkit-type malware from gaining a foothold on the endpoint, we recommend that you do not change this setting.[3]

Note! It is recommended that you do not turn off the operating system's default protection settings. Changing them can have implications for the security level of endpoints.

Hard Disk Encryption

01

The Hardening Principle: Endpoints in general and laptops in particular are at high risk of theft, loss, or being misplaced, which could allow an unauthorized entity to access the information stored in them. Disk encryption renders the information in it unreadable to those who do not hold the encryption key and significantly reduces the risk of information leaks.

02

The Hardening Process: For endpoint owners running the Microsoft Windows operating system, the manufacturer provides disk encryption software called **BitLocker**. Other manufacturers also provide such solutions.

For owners of endpoints operating with Linux, there is an open source disk encryption tool.

Similarly, Apple provides a solution called **FileVault** for disk encryption on computers based on its operating system.

Note! Make sure that the solution encrypts the entire disk to ensure that no information is leaked in case of theft or loss of the endpoint.

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 > Group: **Encryption >** 8.7

Reducing Permissions

01

The Hardening Principle: Accounts with broad permissions (privileged/admin accounts) are among the main targets of cyberattackers since they allow those who gain access to them to take over the endpoint and from there take over the entire network. One of the first measures to reduce the attack surface is to create a regular user account with limited privileges which will be used for daily work.[4]

An account with admin privileges will only be used when needed, such as when installing software. This is because if malware or an attacker accesses the endpoint, using a limited-permissions user makes it difficult for the attacker to gain administrator permissions, make extensive system changes, and be based in the endpoint.

[3] **https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/disabling-secure-boot**.

[4] CIS Control 6: **https://www.cisecurity.org/controls/access-control-management**.

02

The Hardening Process:

- Reduce the number of administrator accounts at the endpoint to the minimum possible (see later section **Hardening Local Administrator at Endpoints** on how to set up an administrator account).
- Do not define the endpoint owner as a local administrator, but as a "regular" user.
- A user must perform every action on the endpoint with the lowest permissions that allow the operation to be performed. In the case of actions that require the use of a privileged user, only the specific action will be performed. Permission-enhancing systems can be used on demand.
- Monitor and provide alerts of any changes or additions to privileged accounts.

Note! The permissions in the organization should be adjusted as needed for the various positions (and a minimum of permissions should be given for each position).

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 > Group: **Access Control >** 4.9, 4.10

Password Policy

01

The Hardening Principle: One of the most common techniques that malicious entities use to hack the organization is an attempted attack or hacking of the intranet's password mechanism.

Bypassing the password mechanism will reduce the need to invest resources and time to hack other mechanisms, such as permissions, systems, and encryption. Therefore, the aim is to make it more difficult for the attacker to attempt to bypass the password mechanism.

A hard-to-crack password will make it difficult for an attacker to guess it within a reasonable amount of time. Choosing a good password will leave the hacker no choice but to try all possible passwords using a brute-force search, thus increasing the time required to run it or keeping the hacker out completely.

Key terminology

The term "brute force" refers to a process or algorithm which operates in a manner of trial and error of all the possibilities for solving a given problem until a correct solution is found.

Using software to guess a user's password is also called a "dictionary attack." This is an attempt to guess the user's password by brute force—that is, trying and checking all the possible passwords or the most likely or most common passwords, usually using files that contain long lists of these types of passwords. An attacker could find such lists online.

02

The Hardening Process: Here are some basic rules for choosing a password.

- As a general rule, do not rely solely on the pasword. It is advisable to incorporate an additional authentication mechanism, such as two-step authentication.[5]
- Do not use the user's details in the password, such as: first name, last name, date of birth, ID card, telephone number, etc.
- Create a password of at least eight characters.
- The password should contain letters, special characters, and numbers.
- Avoid standard words.
- The organization's procedures must state that the password is personal and must not be shared or passed onto anyone inside or outside the organization.

Note: There are various approaches and recommendations, such as the NIST passphrase recommendations.[6]

Policy to enforce on password change:

- Change passwords every 90 days.
- Do not repeat previously used passwords.
- Set user lock after five failures.

Ensure that the network administrator applies the password policy set by the organization at the domain level and use group policy objects (GPOs) to enforce it throughout the intranet.

Quarterly checks, which can be performed by the information security officer or the help desk team for the Active Directory (AD) policy, to verify that the user complies with the policy:

- **Password Required** field: Ensure that all users are required to identify themselves with a password.
- **Password Last Changed** field: Check that there are no password records where the date is more than 90 days in the past.
- **Password Expires** field: Locate users with a configuration that does not require a password change.

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 **>** Group: **Access Control >** 4.35

Note! It is important to make sure that the password management process in the organization complies with the password policy established in order to make it more difficult to hack into the organization and prevent the misuse of this data.

[5] For more information, see the document ***Advanced Multi-Factor Authentication against Cybersecurity Threats*** soon available within this "Cybersecurity Best Practices" collection.

[6] **https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd**

Hardening Local Administrator at Endpoints

01

The Hardening Principle: Local admin permissions on endpoints allow almost complete control over workstations, exposing the intranet to higher risk.

A local admin can access every file and application on the network. When it encounters any permissions issue, it can grant itself the requested permission without any control from the network administrator. The risk is that the endpoint is exposed to any action that the attacker chooses to perform.

Operating systems usually automatically create an admin account. Attackers recognize this account, and it is a weak spot of the organization.

Important! Before disabling or renaming an admin account, ensure the existence of another username with strong permissions for whenever needed.

02

The Hardening Process: An admin account can be hardened in several ways:

- Manually - In small organizations it is possible to set for each endpoint an alternate username for a local administrator.
- By running a script after installation.[7]
- By using GPOs.

Honeypot User

01

The Hardening Principle: A honeypot user is a fictitious user, located in the corporate network with fictitious user information, whose job it is to lure a potential attacker to access the "honey trap."[8]

[7] To do so, you can follow the steps described in: **https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.localaccounts/rename-localuser?view=powershell-5.1&viewFallbackFrom=powershell-5.1localuser%3Fview%3Dpowershell-5.1**.

[8] **https://www.linkedin.com/pulse/honeypots-security-managers-guide-ismail-orhan-ceh**

An attacker who tried to hack into an organization would usually try to locate as many usernames as possible to obtain a selection of connection permissions to the organization, in order to reach a username with high privileges. A honeypot user is meant to lay a trap for the attacker. When they fall into it, an alert will be triggered. In order for this user to be effective, connecting/identifying with the honeypot username must not be enabled; thus, when an identification attempt is made, an alert will be received immediately, making it possible to identify this with near certainty as an attempt to infiltrate the organization.

02

The Hardening Process: The following are steps that must be taken to define a honeypot user:

- First, create a honeypot username that is credible but do not allow any user to connect using this username (inclusively).[9]
- Create a honeypot users and domain users.
- Give the honeypot user all the legitimate permissions in the organization, so that the username does not arouse suspicion with the attacker.
- Set the honeypot username in a software designed to detect activity of said honeypot username, so that the software will send an alert upon connection.

Note!

Using a honeypot user can help the organization shorten the time it takes to detect an attack. This is on the condition that it is planned correctly and that there is a process of monitoring and maintaining the "trap" environment.

The more honeypot usernames the organization uses, the more likely it is to detect an attack.

[9] **https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey.pdf**

/03. Data Protection

Data Backup

01

The Hardening Principle: As mentioned, endpoints in organizations can contain a lot of sensitive information and can therefore be harmed by human error (accidental deletion of information) or by a cyberattack. One of the most common attacks is ransomware, or harmful files that disable information existing in the endpoint by encrypting it. The attackers will not allow access to the information until the ransom is paid. Sometimes even after payment, access to the information is not possible and the information is lost.

In addition to using antivirus software, the most effective way to deal with this type of attack is to back up information. All information essential to the organization must be backed up by means that enable its recovery in the event of damage to an endpoint.[10]

02

The Hardening Process: The way to deal with ransomware attacks is to back up the information by using external means, such as a network drive, an external drive, or cloud backup. The device must be connected to the endpoint only during the backup, and the rest of the time it must be permanently disconnected from the endpoint to prevent it from being damaged in the event of a harmful file penetration.

03

Important Measures

- Assign dedicated physical means for the purpose of backup, such as a server, cloud storage, or network drive.
- Define an individual or team as being responsible for backing up the information in the organization.
- Define a policy for periodic information backup (daily, weekly, monthly) in the organization.
- Perform a recovery test to verify that the backup is effective.

Note! Backing up information will help the organization recover if business information is lost and will contribute to business continuity.

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 > Group: **Business Continuity**

Data Leak Prevention

01

The Hardening Principle: Employees in the organization can take sensitive information out of the organization by various means, such as email, copying to a USB device, and others. Sensitive information can be leaked intentionally or as a result of human error. Therefore, a layer of security against data leakage from the organization is essential. Data leak prevention (DLP) solutions help the organization monitor data according to a predetermined policy consisting of blocking the transfer of information to unauthorized parties, thus minimizing the loss or leakage of sensitive data.[11]

A DLP system can also document user activities on the endpoint and examine suspicious activity that could damage the organization, such as selling information, committing fraud, and other malicious actions.

02

The Hardening Process: The following actions should be considered.

- Establish monitoring policies and relevant rules.
- Monitor access to the organization's sensitive and confidential information.

[10] CIS Control 11: **https://www.cisecurity.org/controls/data-recovery**.

[11] CIS Control 3: **https://www.cisecurity.org/controls/data-protection**.

- Monitor the transfer of data from the endpoint to an external device or an external email address.
- Install DLP systems.

Blocking Devices

01

The Hardening Principle: The use of USB memory devices is common today. These and other removable devices enable information to be quickly copied from a PC to external drives.

These devices can also be used to inject malware/virus into any computer with a USB connection. To protect the sensitive information of the organization, the ability to connect such devices should be restricted at the endpoint.

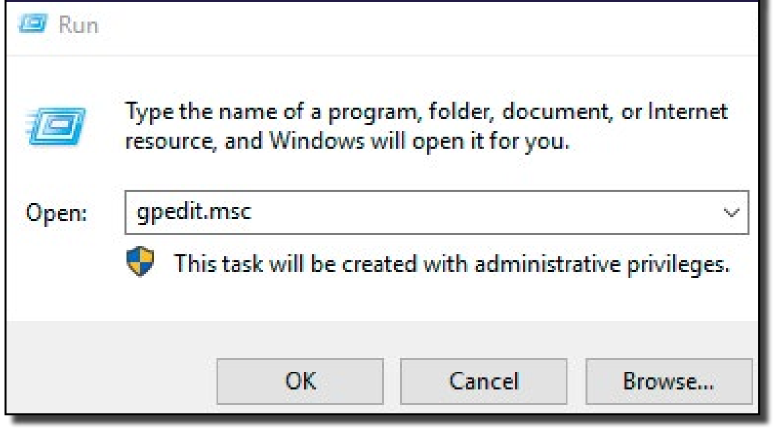
There are two weak spots where it is advisable to protect the endpoint: the computer and any external drives or devices used.

02

The Hardening Process: There are a number of processes available. First is hardening USB connections using the computer's operating system.

- First press the `Start` button and then, in the search bar, type: `run`.
- In the window that opens, enter the command: `gpedit.msc` and then click `OK`.

Figure 3. Process of hardening USB connections via the operating system



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

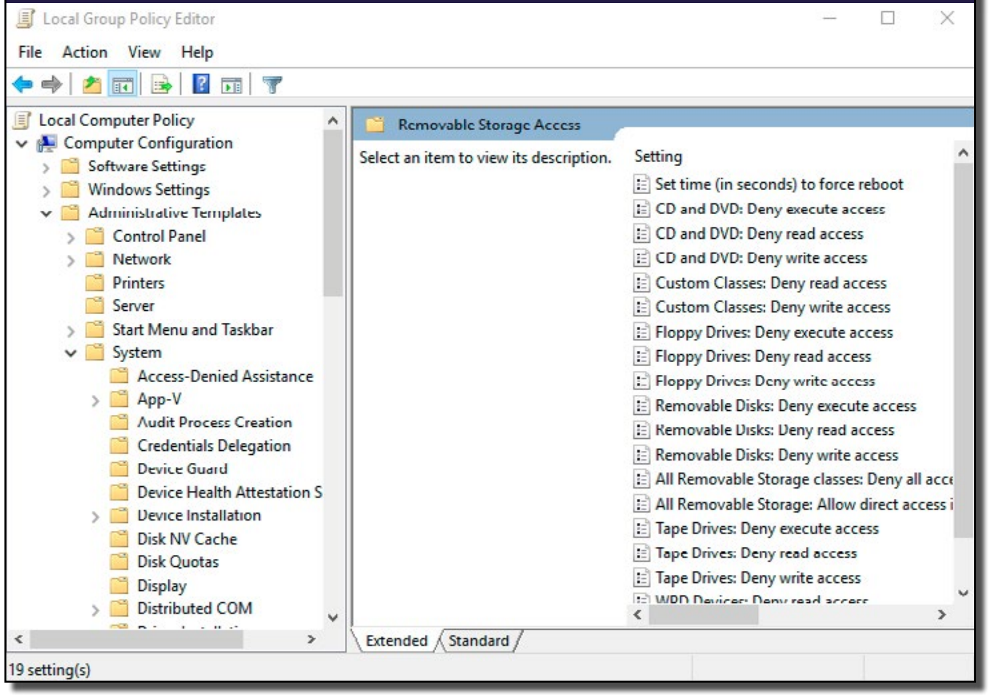
Open: gpedit.msc

This task will be created with administrative privileges.

- In the window that opens, navigate to `Computer Configuration` > `Administrative Templates`.
- Within the `Administrative Templates` folder, first select the `System` folder, then select the `Removable Storage Access` option.
- A set of options will now appear on the right side of the window. One at a time, you must double-click and then configure each of the following options:

`Removable Disks: Deny execute access`
`Removable Disks: Deny read access`
`Removable Disks: Deny write access`

Figure 4. Settings to be configured to harden USB connections



Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Access-Denied Assistance
App-V
Audit Process Creation
Credentials Delegation
Device Guard
Device Health Attestation S
Device Installation
Disk NV Cache
Disk Quotas
Display
Distributed COM

Removable Storage Access

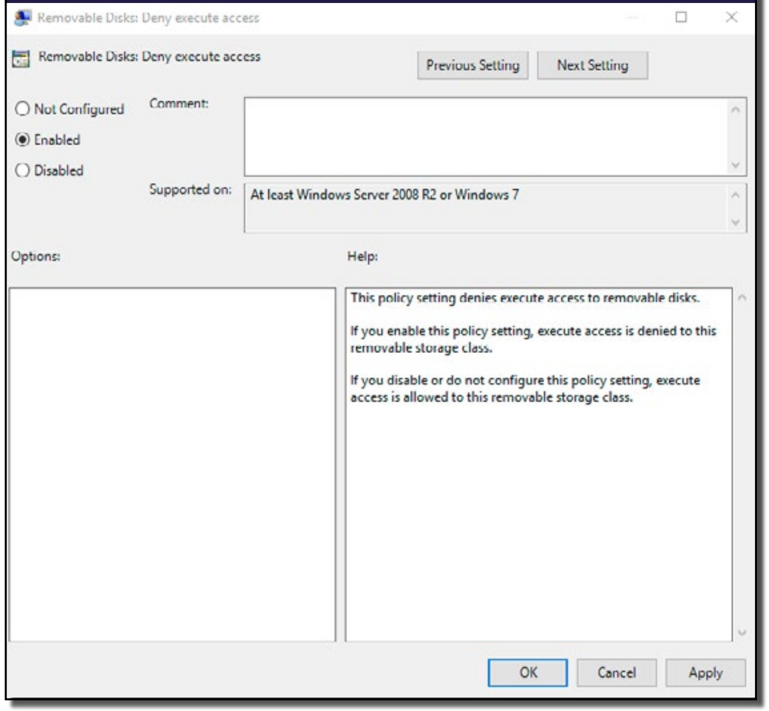
Select an item to view its description.

Setting
Set time (in seconds) to force reboot
CD and DVD: Deny execute access
CD and DVD: Deny read access
CD and DVD: Deny write access
Custom Classes: Deny read access
Custom Classes: Deny write access
Floppy Drives: Deny execute access
Floppy Drives: Deny read access
Floppy Drives: Deny write access
Removable Disks: Deny execute access
Removable Disks: Deny read access
Removable Disks: Deny write access
All Removable Storage classes: Deny all acce
All Removable Storage: Allow direct access i
Tape Drives: Deny execute access
Tape Drives: Deny read access
Tape Drives: Deny write access
WPD Devices: Deny read access

19 setting(s)

- After selecting an item, in the next window, select the `Enabled` option, then click the `OK` button.

Figure 5. Hardening USB connections via the operating system



Removable Disks: Deny execute access

Removable Disks: Deny execute access

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

Help:

This policy setting denies execute access to removable disks.

If you enable this policy setting, execute access is denied to this removable storage class.

If you disable or do not configure this policy setting, execute access is allowed to this removable storage class.

- When this has been completed for all three items, restart the computer.

The second is physical removal:[12]

- Another option is to remove or physically block disk drives and USB ports.

Third is external device protection:

- `AutoRun` - This setting automatically activates files from external or removable devices or opens an options menu. In practice, the device contains a file called `autorun.inf`, in which attackers can plant harmful files which will be triggered by running all the files listed in the `AutoRun` file automatically.

[12] In fact, any unnecessary interface on the computer can be blocked by physical means.

Therefore, it is important to harden `AutoRun` as follows:

- In Microsoft domain-based networks, device blocking can be set in the GPO.

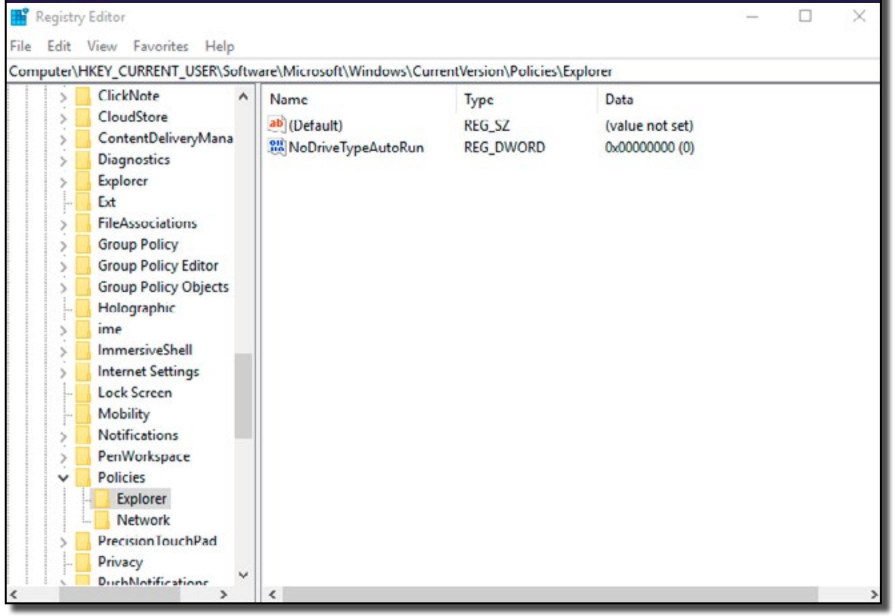
In addition, the endpoint can be hardened locally as follows:

- Click on the `Start` button and type `run` in the search bar.
- In the window that opens, type `regedit` and then click `OK`.
- Access the following path:

  `Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`

- Right-click on the `NoDriveTypeAutoRun` option and then select the `Modify` option.
- In the `Value data` row, change the value to `0xFF` and then click `OK`.
- Restart the computer.

Figure 6. AutoRun hardening



Registry Editor

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Name	Type	Data
(Default)	REG_SZ	(value not set)
NoDriveTypeAutoRun	REG_DWORD	0x00000000 (0)

Note that it is also possible to block only certain files depending on their source by using the values provided in Table 1.

Table 1. Values for locking of AutoRun files

Value	Meaning
0x1 or 0x80	Disables AutoRun on drives of unknown type
0x4	Disables AutoRun on removable drives
0x8	Disables AutoRun on fixed drives
0x10	Disables AutoRun on network drives
0x20	Disables AutoRun on CD-ROM drives
0x40	Disables AutoRun on RAM disks
0xFF	Disables AutoRun on all kinds of drives

03

External Device Scan: It is recommended to always scan an external drive or device before copying files to or from it, and especially before activating files from it. If the antivirus software installed in the organization allows it, it is recommended to set up an automatic scan of any device that is plugged in to the computer.

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 > Group: **Media Security** > 15.5

/04. Security Software

Antivirus[13]

01

The Hardening Principle: The purpose of the antivirus software is to detect virus-type attacks and other harmful files on the endpoint and to defend against their activity.

In optimal condition, the software will be able to detect an attack attempt on the endpoint before the malicious entity can install on the computer.

In another case, where the workstation is already "contaminated" with a malicious file, the antivirus can detect the existing file while it is running on the computer with the help of various signatures (and in some cases even remove it). Therefore it is very important to keep antivirus software updated.

02

The Hardening Process

- Install antivirus software from a reliable supplier at the endpoint.
- Update the antivirus software automatically or proactively (at least once a day or according to the manufacturer's recommendations).

[13] CIS Control 10: **https://www.cisecurity.org/controls/malware-defenses**.

Key terminology

Sandbox: An emulation tool by which the antivirus software analyzes a file or process on a computer, in a quarantine area of computer memory. When the virus is in the quarantine area, it cannot harm and it is possible to check what the results of its activation will be in an isolated manner. If the file is detected as a virus, the antivirus software blocks it and notifies the user.

File Signature: The signature can be a static signature, which is a hash value of a piece of code unique for the virus, or a behavior-based signature—that is, if a software tries to perform any actions defined by the antivirus as suspicious, it must stop and notify the user.

Generic Detection: The antivirus software analyzes the behavior of the processes running on the computer, including monitoring their activity, testing the attempts of a process to access other processes, accessing resources, and so on. When a particular process starts modifying a system file, the antivirus software carefully monitors its behavior.

EDR System

01

The Hardening Principle: Endpoint detection and response (EDR) refers to a category of tools and solutions designed to locate and monitor information at endpoints in the organization. The system works with the help of an agent installed on the endpoints. The agent examines the possibility of external attacks and internal threats by monitoring network traffic and endpoint activity, running services and processes, and others. The agent collects the relevant information and stores it in a predefined database.

An information security staff member who works with the system can use the information collected to identify anomalies, investigate, report, and send alerts about information security incidents in the organization. The uniqueness of this solution is that it is a single platform that protects laptops, desktop computers, servers, and virtual environments.

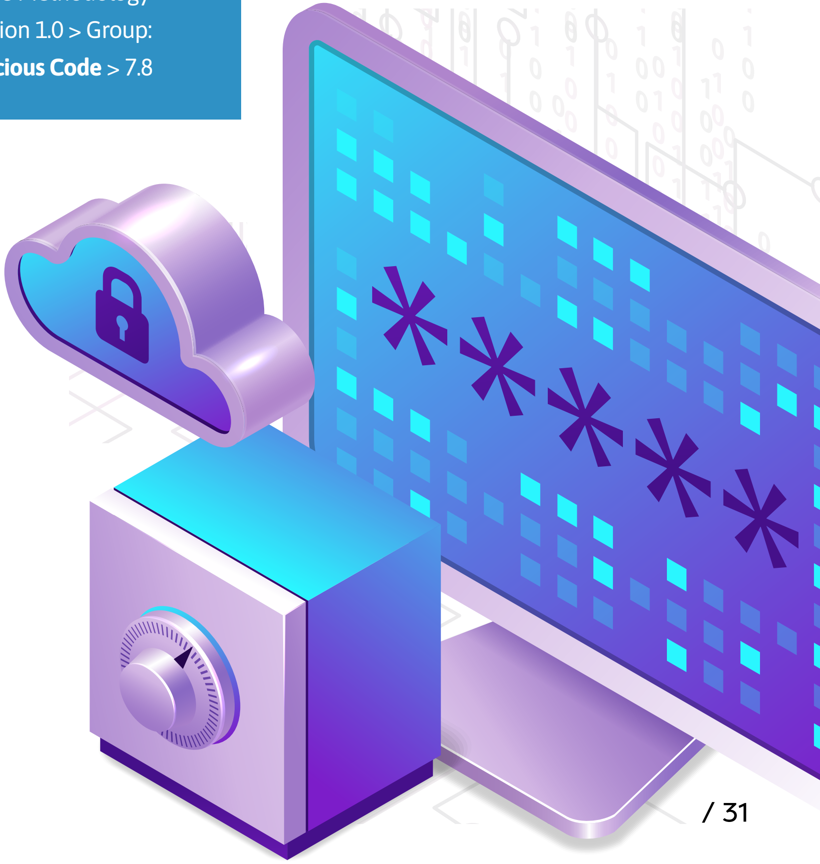
Monitoring endpoints and a short response time to an attack are key to keeping an endpoint secure. EDR solutions can detect a cyberincident or threat on a large number of workstations.

02

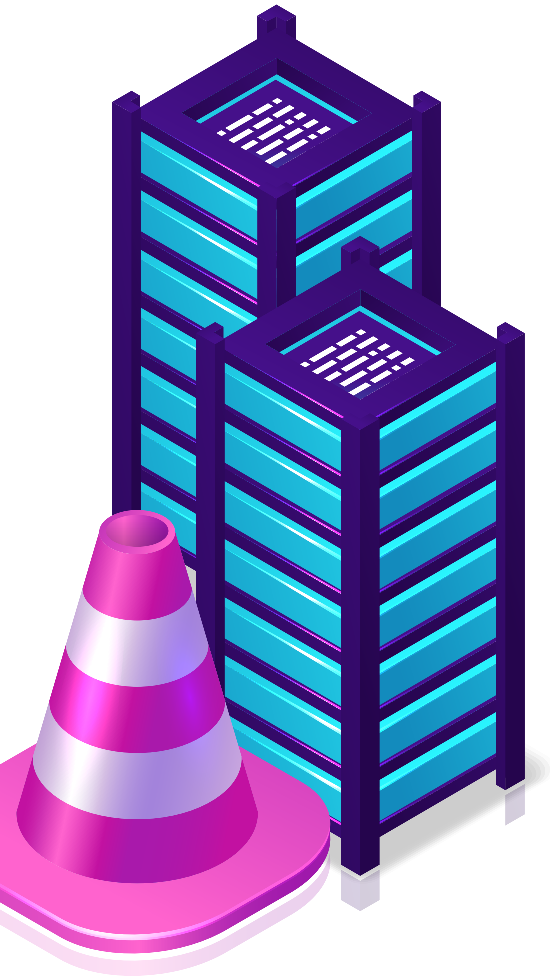
The Hardening Process: The EDR system should be designed in a way that locates the chain of events and stores them for future research and comparison to online events such as behavioral analysis. The emphasis is on settings that will enable false positives to be detected and prevented.

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 > Group: **Preventing Malicious Code** > 7.8

Note! The EDR solution will monitor the activities at the endpoints and will enable the investigation of information security incidents.



/05.
Local Firewall



01

The Hardening Principle: Endpoint operating systems usually provide a firewall that enables illegal traffic to and from the endpoint to be blocked.[14]

The firewall is designed to protect the network by detecting and blocking unauthorized traffic. It also helps block malware, such as viruses and harmful files.

[14] CIS Control 13: **https://www.cisecurity.org/controls/network-monitoring-and-defense**.

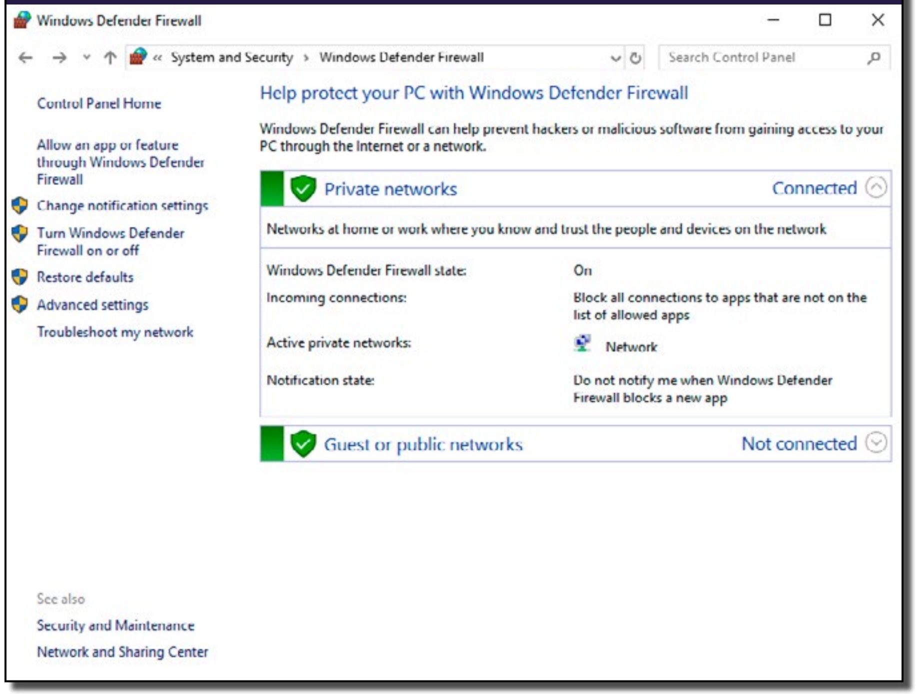
Note! It is important to run the firewall on the endpoints even if your intranet already has a firewall installed, as this is an additional layer of security.

02

The Hardening Process: To verify that the firewall is indeed running in the background, perform these actions in the following order.

- Click the `Start` button and type `Control Panel` in the search bar. Next, access the firewall by selecting `System and Security` > `Windows Defender Firewall`.

Figure 7. Local firewall in Windows



Windows Defender Firewall

« System and Security › Windows Defender Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Security and Maintenance

Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

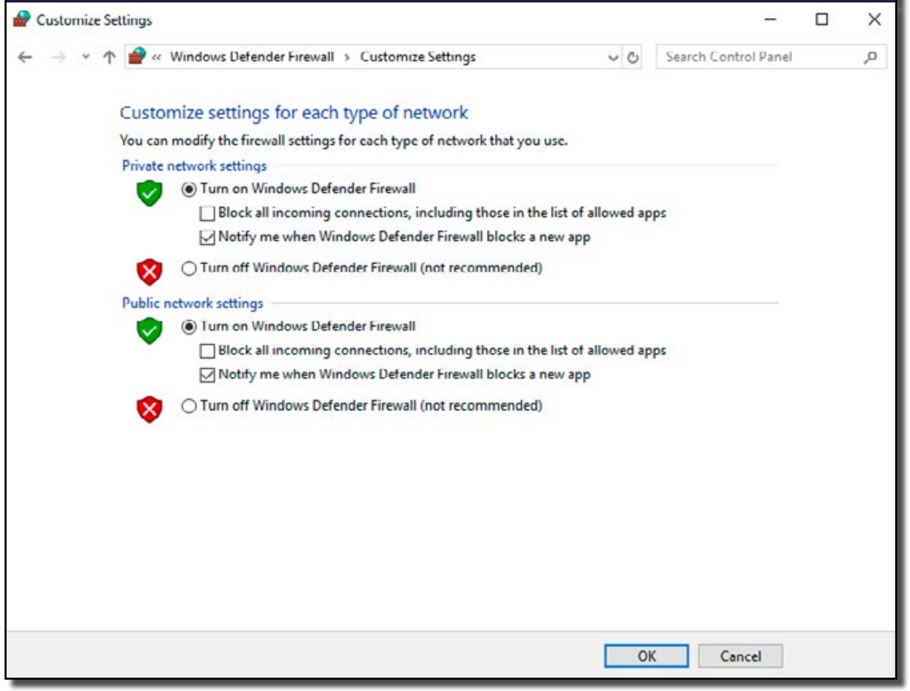
Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Do not notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected

- Select the option: `Turn Windows Defender Firewall on or off`, on the left side of the screen (see Figure 7).

- Make sure the firewall is turned on for both private network and public network settings as shown in Figure 8.

Figure 8. Firewall verification



Customize Settings

« Windows Defender Firewall › Customize Settings

Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 > Group: **Protection of Workstations and Servers** > 6.1

- If necessary, Windows Firewall has three profiles for different environments: `PUBLIC`, `PRIVATE`, and `DOMAIN`.[15]

[15] For more information: **https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-profiles**.

/06. Security Updates

01

The Hardening Principle: In every software, vulnerabilities that hackers can exploit to attack the endpoint are sometimes discovered. Most software suppliers provide security updates for their products to help their customers maintain secure endpoints. In particular, manufacturers of operating systems, which are the key software component at each endpoint, provide security updates on a regular basis (usually once a month) and sometimes distribute critical updates even more frequently. Regular updates minimize the possibility that an attacker can exploit these vulnerabilities.[16]

02

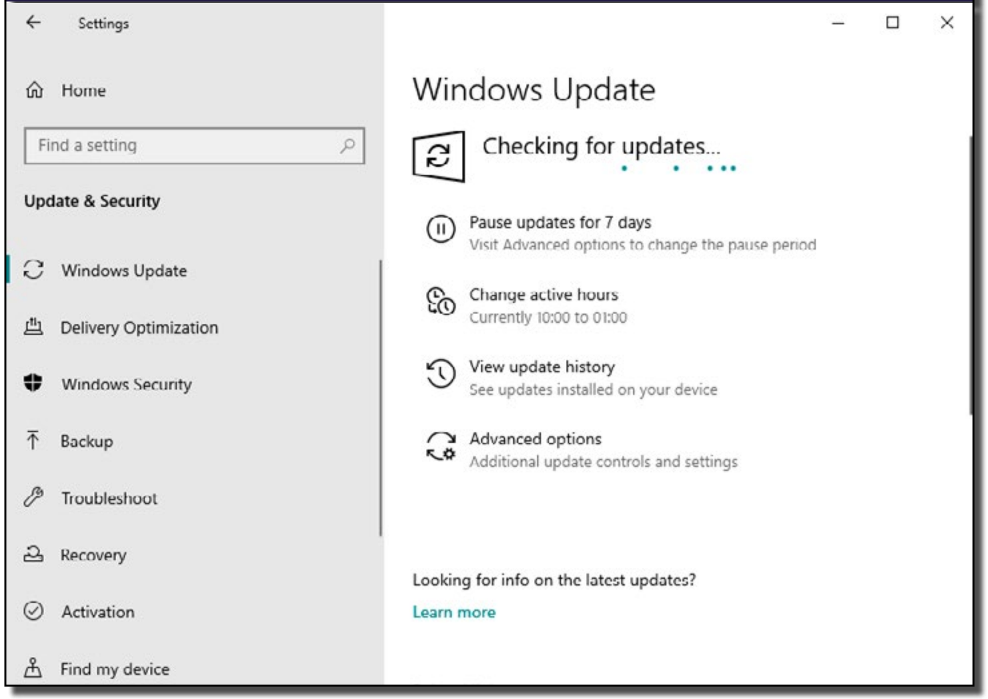
The Hardening Process: As a general rule, updates should be installed automatically without user intervention. However, in doing so there is a risk that an update will disable the endpoint for various reasons. In organizations where the severity of this risk being realized is critical, updates should be made manually and only after it has been verified that they are not disabling endpoints.

[16] CIS Control 7: **https://www.cisecurity.org/controls/continuous-vulnerability-management**.

Follow these steps to perform security updates on the operating system:

- Click the **`Start`** button, and then go to **`Settings`** > **`Update & Security`** > **`Windows Update`**.
- Choose the **`Check for Updates`** option.

Figure 9. Windows update settings



Windows Update

Checking for updates...

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 10:00 to 01:00

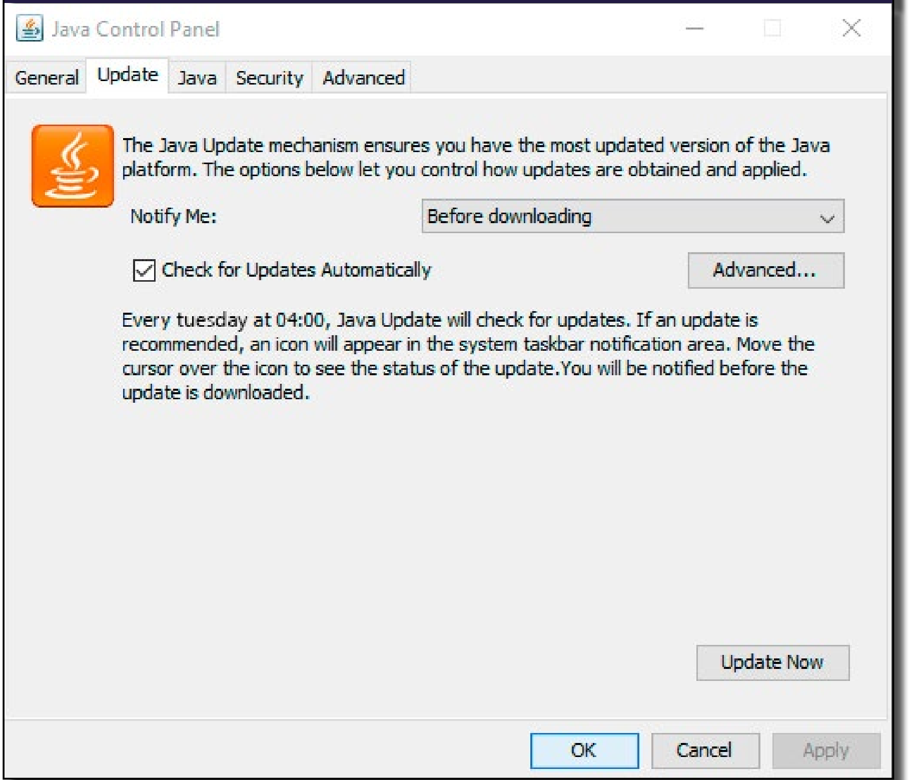
View update history
See updates installed on your device

Advanced options
Additional update controls and settings

Looking for info on the latest updates?
Learn more

Comparably, for standalone programs, you may read the documentation included with the software or simply explore the program's menus to learn how to run the update process or to enable automatic updates if possible (see Figure 10 for an example).

Figure 10. Standalone program (in this case, Java) update settings



The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied.

Notify Me: Before downloading

☑ Check for Updates Automatically

Every tuesday at 04:00, Java Update will check for updates. If an update is recommended, an icon will appear in the system taskbar notification area. Move the cursor over the icon to see the status of the update.You will be notified before the update is downloaded.

Note! Updates to endpoints should be made regularly to prevent attackers from exploiting these vulnerabilities.

For further information on this topic, see Cyberdefense Methodology for an Organization 1.0 > Group: **Preventing Malicious Code** > 7.9

Appendix

Table A1.1. Recommended checklist

Task	Done	Partially Done	Not Done
Physical security of endpoint	□	□	□
BIOS hardening	□	□	□
Hard disk encryption	□	□	□
Admin account hardening	□	□	□
Password policy	□	□	□
Local admin cancellation	□	□	□
Honeypot trap installation	□	□	□
Data backup	□	□	□
Data leakage prevention	□	□	□
Blocking devices	□	□	□
Antivirus software installation	□	□	□
EDR system installation	□	□	□
Local firewall activation	□	□	□
Security updates activation	□	□	□

The endpoint is the computer on which the user of the organization works. Through it, the employee accesses software, applications, and organizational information resources and uses them to perform processes. As such, an endpoint is exposed to a variety of cyberthreats related to the employee's use of the workstation, its settings, and its connection to the organizational network. This document, based on the **Cyberdefense Methodology for an Organization 1.0**[17] published by the National Cyber Directorate, specifies defense recommendations for endpoints.

[17] **https://www.gov.il/en/pages/cyber_security_methodology_for_organizations**

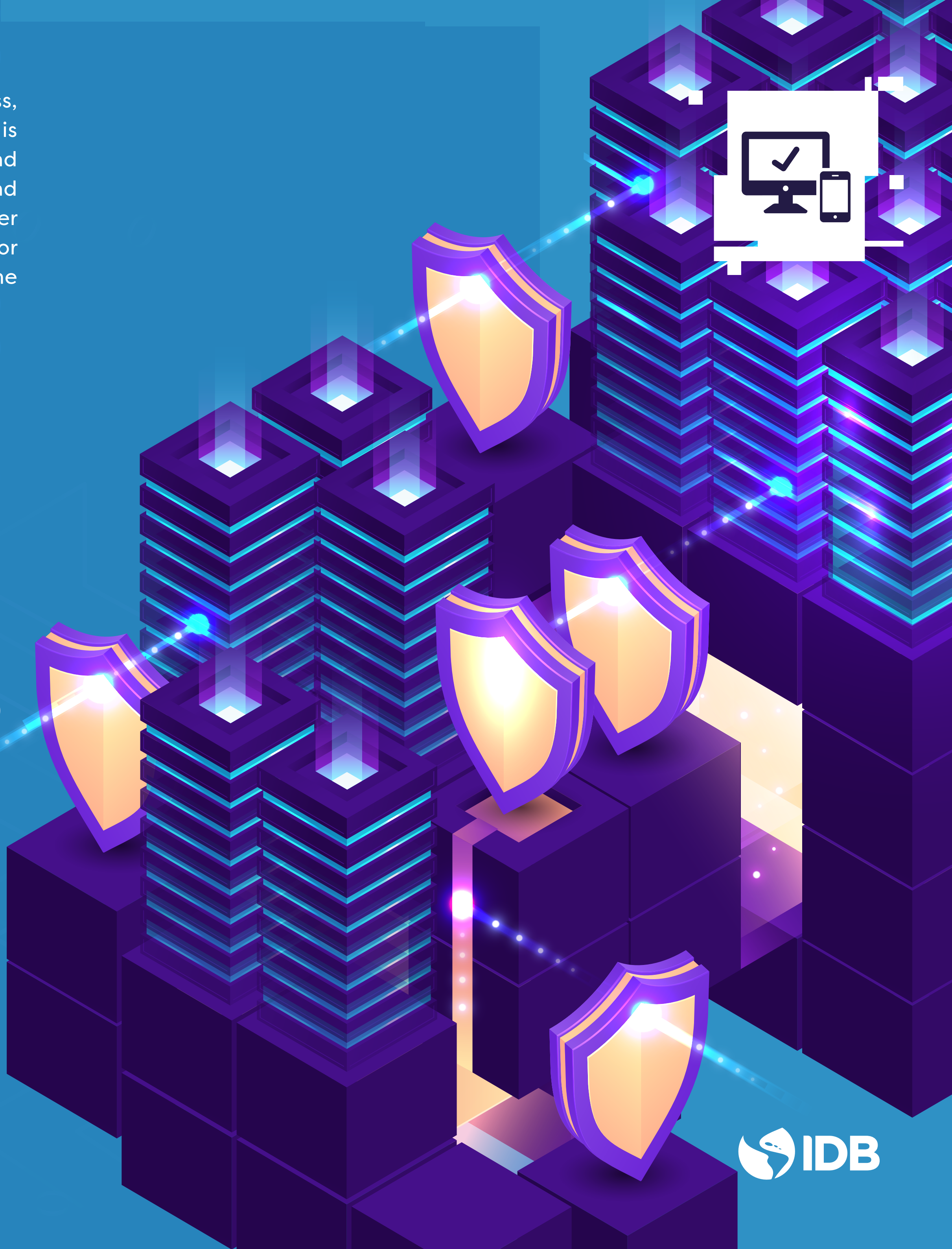
Cyberspace is a field of opportunities in terms of technological progress, connectivity, integration, and global connection to the internet. But it is also a field of threats and risks. Cyberattacks can harm organizations and inflict significant financial and image damage. To be prepared to defend against 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

Volume C: Secure software development



IDB