Security requirement

Microsoft IIS

Deutsche Telekom Group

Version	7.0
Date	Jul 1, 2024
Status	Released

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	3.32	Security requirement
Version	**State**	**Status**
7.0	Jul 1, 2024	Released
Contact	**Validity**	**Released by**
Telekom Security psa.telekom.de	Jul 1, 2024 - Jun 30, 2029	Stefan Pütz, Leiter SEC-T-TST

Summary
This document was created on the basis of the general security policies of the Group and defines the requirements for securely implementing Microsoft IIS web servers. The requirements described in this document shall be met to ensure that a Microsoft IIS web server cannot be easily misused by competent attackers.

Copyright © 2024 by Deutsche Telekom AG.
All rights reserved.

Table of Contents

1. Introduction 4
2. Requirements on web server software 5
3. Configuration requirements 9
4. HTTPS requirements 17
5. Logging 22

1. Introduction

This security document has been prepared based on the general security policies of the Group.
The security requirement is used as a basis for an approval in the PSA process, among other things. It also serves as an implementation standard for units which do not participate in the PSA process. These requirements shall be taken into account from the very beginning, including during the planning and decision-making processes.
When implementing these security requirements, the precedence of national, international and supranational law shall be observed.

2. Requirements on web server software

Req 1	Software and hardware of the system must be covered by security vulnerability support from the supplier.

Only software and hardware products for which there is security vulnerability support by the supplier may be used in a system.
Such support must include that the supplier

- continuously monitors and analyzes the product for whether it has been affected by security vulnerabilities,
- informs immediately about the type, severity and exploitability of vulnerabilities discovered in the product
- timely provides product updates or effective workarounds to remedy the vulnerabilities.

The security vulnerability support must be in place for the entire period in which the affected product remains in use.

Support phases with limited scope of services
Many suppliers optionally offer time-extended support for their products, which goes beyond the support phase intended for the general market, but is often associated with limitations. Some suppliers define their support fundamentally in increments, which may include limitations even during the final phase before the absolute end date of regular support.
If a product is used within support phases that are subject to limitations, it must be explicitly ensured that these restrictions do not affect the availability of security vulnerability support.

Open Source Software and Hardware
Open Source products are often developed by free organizations or communities; accordingly, contractually agreed security vulnerability support may not be available. In principle, it must also be ensured here that the organization/community (or a third party officially commissioned by them) operates a comprehensive security vulnerability management for the affected product, which meets the above-mentioned criteria and is considered to be reliably established.

Motivation: Hardware and software products for which there is no comprehensive security vulnerability support from the supplier pose a risk. This means that a product is not adequately checked to determine whether it is affected by further developed forms of attack or newly discovered vulnerabilities in technical implementations. Likewise, if there are existing security vulnerabilities in a product, no improvements (e.g. updates, patches) are provided. This results in a system whose weak points cannot be remedied, so that they remain exploitable by an attacker in order to compromise the system or to adversely affect it.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.01-1/8.0

Req 2	The software used must be obtained from trusted sources and checked for integrity.

The software used on the system must be obtained from trusted sources and checked for integrity before installation.
This requirement applies to all types of software:

- Firmware and microcode for hardware components
- Operating systems
- Software Libraries
- Application Software

- Pre-integrated application solutions, such as software appliances or containers

as well as other software that may be used.

Trusted Sources

Trusted sources are generally considered to be:

- the official distribution and supply channels of the supplier
- third party distributors, provided they are authorized by the supplier and are a legitimate part of the supplier´s delivery channels
- internet downloads, if they are made from official provisioning servers of the supplier or authorized distributors
  (1) If the provisioning server offers various forms of downloads, those protected by encryption or cryptographic signatures must be preferred to those without such protection.
  (2) If the provisioning server secures the transport layer using cryptographic protocols (e.g. HTTPS, sftp), the associated server certificates or server keys/fingerprints must be validated with each download to confirm the identity of the provisioning server; if validation fails, the download must be cancelled and the provisioning server has to be considered an untrusted source.

Integrity Check

The integrity check is intended to ensure that the received software is free of manipulation and malware infection. If available, the mechanisms implemented by the supplier must be used for checking.
Valid mechanisms are:

- physical seals or permanently applied certificates of authenticity (if the software is provided on physical media)
- comparison of cryptographic hash values (e.g. SHA256, SHA512) of the received software against target values, which the supplier provides separately
- verification of cryptographic signatures (e.g. GPG, certificates) with which the supplier provides its software

In addition, a check of the software using an anti-virus or anti-malware scanner is recommended (if the vendor has not implemented any of the aforementioned integrity protection mechanisms for its software, this verification is mandatory).

Extended integrity checking when pulling software from public registries

Public registries allow developers to make any of their own software projects available for use. The range includes projects from well-known companies with controlled development processes, as well as from smaller providers or amateur developers.
Examples of such registries are:

- Code registries (e.g. GitHub, Bitbucket, SourceForge, Python Package Index)
- Container registries (e.g. Docker Hub)

Software from public registries must undergo an extended integrity check before deployment.
In addition to the integrity check components described in the previous section, the extended check is intended to explicitly ensure that the software actually performs its function as described, does not contain inherent security risks such as intentionally implemented malware features, and is not affected by known security vulnerabilities. If the software has direct dependencies on third-party software projects (dependencies are very typical in open source software), which must also be obtained and installed for the use of the software, these must be included in the extended integrity check.

Methods for an extended integrity check can be, for example:

- Strict validation of project/package names (avoidance of confusion with deliberately imitated malicious software projects)
- dynamic code analysis / structured functional checks in a test environment
- static code analysis using a linter (e.g. Splint, JSLint, pylint)
- Examination using a security vulnerability scanner (e.g. Qualys, Nessus)
- Examination using a container security scanner (e.g. JFrog Xray, Harbor, Clair, Docker Scan)

- Examination using an SCA (Software Composition Analysis) tool or dependency scanner (e.g. OWASP Dependency Check, Snyk)

The test methods must be selected and appropriately combined according to the exact form of software delivery (source code, binaries/artifacts, containers).

Motivation: Software supply chains contain various attack vectors. An attacker can start at various points to manipulate software or introduce his own routines and damage or control the target environment in which the software is subsequently used. The attack can occur on the transport or transmission path or on the provisioning source itself. Accordingly, an attack is facilitated if software is not obtained from official and controlled sources or if an integrity check is omitted.
There is a particular risk for software obtained from public registries, as these are open to anyone for the provision of software projects. Perfidious attack methods are known, in which the attacker first provides completely inconspicuous, functional software for a while and as soon as it has established itself and found a certain spread, deliberately hidden malicious code is integrated in future versions. Other methods rely on similar-sounding project names for widely used existing projects or overruling version numbers to inject manipulated software into any solutions based on them.

Implementation example: Obtain the software via the official delivery channels of the supplier. Upon receipt of the software, immediately check for integrity using cryptographic checksums, as provided by the supplier, as well as scan for any infections by known malware using anti-malware / anti-virus scanners. Storage of the tested software on an internal, protected file storage and further use (e.g. rollout to the target systems) only from there.

For this requirement the following threats are relevant:
- Unauthorized modification of data
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.01-2/8.0

Req 3	Known vulnerabilities in the software or hardware of the system must be fixed or protected against misuse.

Known vulnerabilities in software and hardware components must be fixed by installing available system updates from the supplier (e.g. patches, updates/upgrades). Alternatively, the use of workarounds (acute solutions that do not fix the vulnerability, but effectively prevent exploitation) is permissible. Workarounds should only be used temporarily and should be replaced by a regular system update as soon as possible in order to completely close the vulnerabilities.

Components that contain known, unrecoverable vulnerabilities must not be used in a system.

The treatment of newly discovered vulnerabilities must also be continuously ensured for the entire deployment phase of the system and implemented in the continuous operating processes of security patch management.

Motivation: The use of components without fixing contained vulnerabilities significantly increases the risk of a successful compromise. The attacker is additionally favored by the fact that, as a rule, not only detailed information on vulnerabilities that have already become known is openly available, but often also already adapted attack tools that facilitate active exploitation.

Implementation example: Following the initial installation of an operating system from an official installation medium, all currently available patches and security updates are installed.

Additional information:
The primary sources of known vulnerabilities in software/hardware are lists in the release notes as well as the security advisories from the official reporting channels of the supplier or independent CERTs. In particular, the reporting channels are sensibly integrated into continuous processes of security patch management for a system, so that newly discovered vulnerabilities can be registered promptly and led into operational remedial measures.
As a complementary measure to the detection of potentially still contained types of vulnerabilities that have in principle already become known, targeted vulnerability investigations of the system can be carried out. Particularly specialized tools such as automated vulnerability scanners are suitable for this purpose. Examples include: Tenable Nessus, Qualys Scanner Appliance.

For this requirement the following threats are relevant:

- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.01-10/8.0

3. Configuration requirements

Req 4	The identity of an application pool must not be a user account with system privileges.

Motivation: If the web server process runs with administrative access rights, an attacker who obtains control over this process would be able to control the entire system.

Implementation example: For IIS 7, IIS 7.5 and IIS 8, an application pool can be configured in the IIS Manager. After the application pool to be configured has been selected, click on “Advanced settings...” in the “Actions” pane. The “Identity” can be found in the “Process Model” section and modified by first clicking in the value field and then clicking on “...”. Neither the built-in accounts “LocalService” or “LocalSystem” shall be selected here nor a custom account with corresponding privileges.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.32-4/7.0

Req 5	The web server service must be bound only to interfaces, which are necessary to connect the service.

In most cases the web server service needs to be bound only to one interface.

Motivation: The more interfaces provide access to the web server, the higher is the attack risk.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

ID: 3.03-5/7.0

Req 6	HTTP methods that are not required must be deactivated.

Standard requests to web servers only use GET and POST. If other methods are required, they must be processed securely. TRACE or TRACK respectively must be deaktivated.

Motivation: HTTP TRACE could be misused by an attacker. This method allows for debugging and trace analysis of connections between the client and the web server. The Microsoft IIS web server uses the TRACK alias for this method. Other HTTP methods could also be used to obtain information about the server, or they could be directly misused by an attacker.

Implementation example: For IIS 7, IIS 7.5 and IIS 8, HTTP methods that are not required can be deactivated for a web site as follows:In the IIS manager select the web site to be configured and then open “Request Filtering” in the “IIS” section of the “Features View”. Then, in the “Actions” pane, select “Edit Feature Settings...” and, if necessary, deactivate the item “Allow unlisted verbs”. Now select the tab “HTTP verbs” and enter all permitted HTTP methods via “Allow Verb ...” in the “Actions” pane.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.32-6/7.0

Req 7	Unless they are required web server role services must not be activated.

If they are not required, the following web server role services must not be activated:

- FTP server
- IIS Management Service for Remote Administration
- All Application Development features (ASP, CGI, ISAPI, Server Side Includes in particular)
- WebDAV Publishing

Motivation: Each Windows feature can have security vulnerabilities and should therefore be deactivated if it is not required.

Implementation example: Using powershell the staus of web server role services may be displayed by the command

Get-WindowsFeature Web*

This command's output especially shows the name of role services as it may be used for further commands.
Unwanted features my be uninstalled by using the command

Uninstall-WindowsFeature <Name>

Names of role services to be uninstalled especially are

- Web-Ftp-Server
- Web-Mgmt-Service
- Web-App-Dev
- Web-DAV-Publishing

For this requirement the following threats are relevant:

- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

ID: 3.32-7/7.0

Req 8	If Server Side Includes (SSI) are active, the execution of system commands must be deactivated.

Motivation: The Server Side Includes (SSI) technology, which is implemented in most web server products as an additionally loadable module, can potentially be used by attackers. The “exec” function of SSI, in particular, could be used to execute system commands, which represents a risk.

Implementation example: The execution of system commands can be deactivated for a web site as follows:
In the IIS Manager select the web site to be configured and then open the “Configuration Editor” in the “Management” section of the “Features View”. Now, in the “system.webServer/serverSideInclude” section, change the value of “ssiExecDisable” to “True”.

Alternatively the following command may be used

Set-WebConfigurationProperty -PSPath 'IIS:\' -location "<web_site>" -filter 'system.webServer/serverSideInclude' -name 'ssiExecDisable' -value 'True'

Replace "<web_site>" with the name of the web site to be configured.
The configuration may also be changed for all web sites:

Set-WebConfigurationProperty -PSPath 'IIS:\' -filter 'system.webServer/serverSideInclude' -name 'ssiExecDisable' -

value 'True'

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 3.32-8/7.0

Req 9	CGI shall not be used.

Motivation: Inapropriate CGI configuration may allow multiple attack vectors. Modern web servers provide safer and more performant alternatives to CGI. Therefore CGI is neither necessary nor recommended.

Implementation example: Using powershell CGI may be deactivated by the command

Uninstall-WindowsFeature Web-CGI

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.32-9/7.0

Req 10	If WebDAV is used for writing files, access must not be granted without successful authentication.

Motivation: WebDav makes it possible to update content online which has been made available by the web server. This function could therefore be misused to change website content.

For this requirement the following threats are relevant:
- Unauthorized modification of data

ID: 3.03-10/7.0

Req 11	If WebDAV ist used, the access to needed directories must be restricted regarding the authorized user.

Access rights to all files accessible by WebDAV must be configures as restrictively as possible. Additionally, if WebDAV is used, WebDAV access must be restricted to the directories required.

Motivation: WebDav makes it possible to update content online which has been made available by the web server. This function could therefore be misused to change website content.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.03-11/7.0

Req 12	Access rights for web server configuration files must only be granted to the owner of the web server processs or a user with system privileges.

Motivation: Configuration files may only be written by the owner of the web server process or a user with system privileges. Otherwise it would be possible for unauthorized users to change the configuration of the web server or to obtain configuration information which could be used for an attack.

Implementation example: Delete “read” and “write” access rights for “others.” Only grant “write” access to the user who configures the web server.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.03-12/7.0

Req 13	If the “Default Web Site” is not used, it must be deleted.

Motivation: The „Default Web Site” is delivered with example files in a standard configuration. If an attacker obtains access to the „Default Web Site”, he can therefore draw conclusions about the system used.

Implementation example: Using IIS Manager right click on the "Default Web Site" and select "Remove".

Alternatively using powershell enter the command

Remove-Website -Name " Default Web Site"

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.32-13/7.0

Req 14	Default files in a website’s directory must be deleted.

A newly created web site's directory may contain default files. Usually this is an index HTML file and an image file, but there may be additional example files or tutorials.These files must be deleted. This concerns, in particular, all files in the directory of the “Default Web Site”, if this web site is used.

Motivation: By using examples, information could be obtained about the installed software (version). Examples can include security vulnerabilities.

Implementation example: After creating a web site delete all files in the web sites main directory.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.32-14/7.0

Req 15	The Windows feature “Directory Browsing” of the Internet Information Services or the “Web Server” role service “Directory Browsing”, respectively, must be deactivated.

Motivation: Directory listings contain information about files and directory structures which could be misused.

Implementation example: Using powershell directory browsing may be deactivated by the following command:

Uninstall-WindowsFeature Web-Dir-Browsing

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.32-15/7.0

Req 16	The HTTP “Server” header must not include information on the software and version of the web server.

Motivation: Any information about the web server could allow conclusions to be drawn about security vulnerabilities.

Implementation example: For IIS 10 the "Server" header may be removed from output by entering the following comman in PowerShell

```
Set-WebConfigurationProperty -PSPath 'IIS:\' -filter
'system.webServer/security/requestFiltering' -name
'removeServerHeader' -value 'True'
```

For older versions of IIS the UrlScan tool,may be used. The entry

```
RemoveServerHeader=1
```

or

```
AlternateServerName=<Webserver>
```

is made in the “[Options]” section of the UrlScan configuration file, whereby <Webserver> can be replaced by the string “Webserver”, for example.

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.32-16/7.0

Req 17	Additional HTTP response headers with information about the software and version of the web server or components used, must not be set.

Motivation: Any information about the web server or the components used could allow conclusions to be drawn about security vulnerabilities.

Implementation example: Using PowerShell all additional response headers may be removed by entering the command

Remove-WebConfigurationProperty -PSPath 'IIS:\' -filter 'system.webServer/httpProtocol/customHeaders' -Name .

Alternatively when using the IIS manager select the server or the web site to be configured and then open “HTTP Response Headers” in the “IIS” section of the “Features View”. Headers which contain non-permissible information such as the “Xpowered- by” header can now be deleted.

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.32-17/7.0

Req 18	Information about the webserver in error pages, that are being delivered by the web server, must be deleted.

Default error pages must be replaced with user-defined error pages.

User-defined error pages must not include version information about the web server and the modules/addons used. Error messages must not include internal information such as internal server names, error codes, etc.

Motivation: Any information about the web server could allow conclusions to be drawn about security vulnerabilities.

Implementation example: In the IIS manager select the server or the website to be configured and then open the “Error pages” in the “IIS” section of the “Features View”. Now either edit the error files under the paths specified here or enter different paths to specific new error pages without information about the web server product and version.
By default, the error pages are defined at server level and then passed on to the individual web sites. If this is not changed, it is therefore sufficient to modify the error files defined at server level.

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.32-18/7.0

Req 19	Unauthorized changes to Web.config files must be prevented.

Microsoft IIS allows for site, application or directory specific configuration in Web.config files. Access rights to these files must be set as restrictive as possible. In particular, these files must not be writable for users without administrative privileges.
Restrictive access rights are already assigned to all Web.config files that have been created by IIS Manager. Especially for (virtual) directories that are integrated into the document tree it is important to make sure that no unauthorized user has the possibility to create or modify those files.

Motivation: A web site’s configuration could be modified by other users with the help of Web.config files. This way, for example, a user could get unauthorized access to a web site’s files.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.32-19/7.0

Req 20	Configurable settings in Web.config files must be as restrictive as possible.

All sections in the central configuration file ApplicationHost.config that refer to security relevant or critical aspects must be locked, unless individual settings on web site level are compulsory. By default this is the case, changes must not be made without legitimate reason.

Motivation: Settings in sections that are not locked may be changed by distributed Web.config files that are located in document directories. This may make it easier for a user to accomplish unauthorized configuration changes.

Implementation example: ApplicationHost.config is located in %windir%\system32\inetsrv\config. The different sections’ properties are defined within a special <configSections> section. A section is locked if its „overrideModeDefault” attribute is set to “Deny”.
For most sections the default value is okay but should be checked. A change is required for section "directoryBrowse". Here the entry must be corrected to

```
<section name="defaultDocument" overrideModeDefault="Deny" />
```

This change my as well be accomplished by entering the following command in PowerShell

```
Set-WebConfigurationProperty -PSPath 'IIS:\' -filter 'system.webServer' -name 'sections[directoryBrowse].overrideModeDefault' -value Deny
```

The current setting can be viewed by issuing the following command

```
Get-WebConfigurationProperty -PSPath 'IIS:\' -filter 'system.webServer' -name 'sections[directoryBrowse].overrideModeDefault'
```

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.32-20/7.0

Req 21	The web server may only deliver files which are meant to be delivered.

Restrictive access rights must be assigned to all files which are directly or indirectly (e.g., via links or in virtual directories) in the web server's document directory. In particular, the web server must not be able to access files which are not meant to be delivered.
For IIS, in particular virtual directories used to integrate the content of other applications, for example, must be thoroughly configured.

Motivation: If additional files or directories are integrated via links or virtual directories into the document directory of the web server, in particular, it is possible that a user can access files via the web server which he should not be allowed to view. This must be prevented through careful configuration.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

ID: 3.32-21/7.0

Req 22	The web server must be robust against overload situations.

A web server must provide security measures to deal with overload situations. In particular, partial or complete impairment of web server availability must be avoided. Potential protective measures include:
- Restricting the maximum number of HTTP sessions per IP address
- Defining the maximum size of a HTTP request
- Defining a timeout for HTTP request

Restrictions must be implemented in consideration of the application to be protected and its characteristics. The following values may be uses as a guideline:

If the web server will not be used for uploads:
- Maximum number of HTTP sessions per IP address: 50
- Maximum size of a HTTP request: 20000 bytes
- Timeout for HTTP requests: 30 seconds

If the web server may also be used for uploads:
- Maximum number of HTTP sessions per IP address: 50
- Maximum size of a HTTP request: 10000000 bytes or, if known, maximum size of expected upload
- Timeout for HTTP requests: 60 seconds or, if known, time to complete maximum upload

Motivation: Attackers often try to bring a web server into an overload situation by using denial-of-service (DoS) attacks. If such an attack is successfull the web server's availability or integrity may be impaired.

Implementation example: In order to restrict the number of HTTP sessions per IP address the required Windows feature or IIS role service "IP and domain restrictions", respectively, must be installed. Installation may be done by enter-

ing the following command in PowerShell

Install-WindowsFeature Web-IP-Security

All necessary configuration my be done from within the IIS manager. The number of HTTP sessions per IP address an the maximum request size may be configured either for the web server or single web sites. The timeout may only be configured for web sites.

To configure the number of HTTP sessions per IP address either select the server or a web site and then open the feature "IP Address and Domain Restrictions". Now within "Actions" click on "Edit Dynamic Restriction Settings...". In the window opening check "Deny IP Address based on the number of concurrent requests".

To configure the maximum HTTP request size either select the server or a web site and then open the feature "Request Filtering". Now within "Actions" click on "Edit Feature Settings...". In the window opening the request size may be configured in the field "Maximum allowed conten length (Bytes)".

To configure the HTTP request timeout select a web site and then within "Actions" under "Configure" click on "Limits...". In the window opening the timeout may be configured in the field "Connection time-out (in seconds)".

The values may be set by using PowerShell as well. Replace <web_site> by the web site's name and <value> by the value to be set in the following commands.

Set values system wide:

Set-WebConfigurationProperty -PSPath 'IIS:\' - filter system.webServer/security/dynamicIpSecurity/denyByConcurrentRequests -name Enabled -value True

Set-WebConfigurationProperty -PSPath 'IIS:\' - filter system.webServer/security/requestFiltering/requestLimits -name maxAllowedContentLength -value <value>

Set-WebConfigurationProperty -PSPath 'IIS:\' - filter 'system.applicationHost/sites/siteDefaults/limits' -name connectionTimeout -value <value>

Set values for a specific web site:

Set-WebConfigurationProperty -PSPath 'IIS:\' -location "<web_site>" - filter system.webServer/security/dynamicIpSecurity/denyByConcurrentRequests -name maxConcurrentRequests -value <value>

Set-WebConfigurationProperty -PSPath 'IIS:\' -location "<web_site>" - filter system.webServer/security/requestFiltering/requestLimits -name maxAllowedContentLength -value <value>

Set-WebConfigurationProperty -PSPath 'IIS:\' - filter 'system.applicationHost/sites/site[@name = "<web_site>"]/limits' -name connectionTimeout -value <value>

For this requirement the following warranty objectives are relevant:
- Integrity
- Availability

ID: 3.32-22/7.0

4. HTTPS requirements

Req 23	Data in need of protection must be protected against unauthorized access and modification during transmission.

The need for protection of data to be transmitted depends on its classification (e.g. according to applicable legal data privacy requirements, regulatory requirements, contractual obligations), the potential damage in the event of its misuse, and other relevant factors (e.g. transmission via public networks). The nature and extent of the protective measures must be appropriately chosen.
Authentication attributes such as passwords or tokens etc. are generally considered to be in need of protection. Data that determines the functionality and security-relevant behavior of a system (e.g. updates & patches, configuration parameters, remote maintenance, control via APIs) are also considered to be fundamentally in need of protection.

Compliance with the protection objectives of confidentiality and integrity must be consistently guaranteed during the transmission of data in need of protection.

As a rule, this requires the implementation of cryptographic methods (e.g. encryption, signatures, Hashes).
Cryptographic methods may

- be applied directly to the data before transmission, which can make subsequent transmission acceptable even via insecure channels
- be used on the transmission channel to create a secure channel and protect any kind of data passing through it
- or be implemented as a combination of both.

Cryptographic methods used for the transmission of data must be recognized and effective for this purpose and must have no known vulnerabilities.

Motivation: The transmission of data without adequate protection enables an attacker to intercept, use, disseminate, modify or remove it from transmission without authorization. This potentially opens up further attack vectors on the immediate target systems as well as connected other systems and can lead to significant failures, loss of control and damage as well as resulting penalty claims and reputational losses towards customers and business partners.

Implementation example: [Example 1]
Confidential documents are encrypted before they are sent by e-mail to the customer.

[Example 2]
An administrator configures a new cloud application over the Internet. Access is via a TLS-encrypted connection ("https").

[Example 3]
A system obtains automatic software updates from an update server. The update server delivers the software updates cryptographically signed. The system can thus validate the received software updates and reliably rule out that they have been manipulated during transmission.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.01-15/8.0

Req 24	For encryption with HTTPS the TLS protocol in version 1.2 or higher must be used.

SSL and TLS 1.0/1.1 must be considered outdated and thus may not be activated or must be deactivated, respectively. TLS in version 1.2 provides a sufficient protocol security and also offers Authenticated Encryption Associated

Data (AEAD) encryption schemes.

Motivation: The current versions of TLS fix previous known security vulnerabilites and attack surfaces on the TLS protocol handshake.

Implementation example: SSL/TLS is configured through corresponding registry entries. The following entries must be made for exclusive use of TLS versions 1.2 and later:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server] "Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Server] "Enabled"=dword:ffffffff

The value of “Enabled” specifies in each case whether the protocol may be used (value not equal 0) or not (value 0). Non-existent keys must be created if necessary.

TLS 1.3 may not be supported on the Windows Server version used. In this case the last entry may be omitted.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.32-24/7.0

Req 25	The web server must be configured in such a way that the use of the latest version of the TLS protocol is enabled.

Motivation: The latest version of the protocol offers the best possible protection and contains fixes to known vulnerabilities in previous versions of the protocol.

Implementation example: Starting with Windows Server 2008 R2 the registry must contain the following entries:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "Enabled"=dword:ffffffff

and, if supported,

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3\Server] "Enabled"=dword:ffffffff

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.32-25/7.0

Req 26	The TLS configuration must use secure cipher suites.

Acceptable cipher suites may only use the following algorithms:

Server/Client Authentication & Key Agreement	Encryption	Message Authentication & Integrity (MAC)
ECDHE_ECDSA ECDHE_RSA DHE_DSS[1] DHE_RSA[1]	AES_128_CBC AES_128_GCM AES_128_CCM AES_192_CBC AES_192_GCM AES_192_CCM AES_256_CBC AES_256_GCM AES_256_CCM CHACHA20_POLY1305	SHA256 SHA384 SHA512 SHA-3-256 SHA-3-384 SHA-3-512

[1]min. 4096-bit Parameter

TLS 1.3 explicitly specifies the usage of only DHE and ECDHE for server/client authentication and key agreement. Thus TLS 1.3 cipher suite notation does not contain an indication in this regard.

By fulfilling this requirement the Perfect Forward Secrecy (PFS) property in the TLS/SSL implementation will be achieved.

Motivation: Cipher suites known to be unsecure do not offer sufficient protection.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.03-23/7.0

Req 27	The TLS configuration must provide that the cipher suite considered most secure is being chosen with highest priority.

Motivation: When a TLS connection is being established a cipher suite is selected based on the cipher suites available both on client and on server side. In order to ensure a high compatibility to all kinds of client systems the web server must not only allow for the cipher suites considered most secure. To make sure that nevertheless for each client the best possible cipher suite is selected and thus the connection is best protected the configuration must contain an according prioritization.

Implementation example: The list of cipher suites as well as their order may edited by using the group policy object editor:

1. At a command prompt, enter gpedit.msc. The Group Policy Object Editor appears.
2. Now expand "Computer Configuration", then "Administrative Templates" and finally "Network". Now click "SSL Configuration Settings".
3. Under "SSL Configuration Settings", double-click "SSL Cipher Suite Order setting".
4. In the "Options" section of the "SSL Cipher Suite Order pane" the cipher suite order may be specified now. Please follow the instructions in the "Help" section. In particular, the string entered may not contain more than 1023 characters.
5. The new settings will take effect after a reboot.

The following cipher suites must be used. The cipher suites are listed from highest priority at the top to the lowest priority at the bottom. For operating systems before Windows Server 2012 the list may have to be shortened.

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.32-27/7.0

Req 28	Certificates must be issued by a certification authority whose certificates are recognized by the commonly used web browsers.

For critical applications that can be used via the Internet, use of an extended validation certificate (EV certificate) is recommended.

Motivation: Only if the certificate authority (CA) is contained in the CA list of the browser being used the browser can verify the authenticity of the server.or web application
Stricter issuing criteria apply to EV certificates. If an EV certificate is used, this is visualized in the browser. Even if EV certificates do not improve security, their use increases the trustworthiness of the server for the user.

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.03-25/7.0

Req 29	Certificates must lose their validity after a maximum of 1 year.

In the case of certificates of an internal CA, in particular for machine interfaces, the period may be extended to a maximum of 3 years.

Motivation: The methods used for analysing and breaking cryptographic processes are improved continuously. Therefore the security of the certificates can be ensured for a limited period only. But, according to a general estimation, the security of the certificates is ensured for the required validity period of one year, if an appropriate key length is used.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.03-26/7.0

Req 30	Certificates must have a key length of at least 3072 bits when using RSA or 256 bits when using ECC.

Remarks on DSA and RSA certificates:
For DSA and RSA, key lengths smaller than 3000 bits may only be used in legacy systems [BSI TR-02102-1] until the

end of 2025 and
should be substituted at the next opportunity. Because of the better performance, elliptic curve (EC-DSA) certificates shall be preferred (if supported and technically doable).
RSA-PKCS#1 v1.5 may only be used in legacy systems and should be (if feasible) substituted at the earliest opportunity [BSI TR-02102-1].

References:
[BSI TR-02102-1] Bundesamt für Sicherheit in der Informationstechnik: Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1, Version 2022-01, 28.01.2022

Motivation: In order to guarantee the security of certificates over the validity period, the cryptographic keys must have an appropriate length. According to a general estimation, a key length of 3072 bits provides sufficient protection for the next years. For ECC algorithms, shorter key lengths already provide the same level of security.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.03-27/7.0

5. Logging

Req 31	Access to the webserver must be logged.

The web server log must contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- URL
- Status code of web server response

Logging must be done considering the currently valid legal, wage and company regulations. This regulations state among others that logging of events can be done only earmarked. Logging of events for doing a work control of employees is not allowed.

Motivation: For the analysis of security incidents it is very important to have basic information on how the attack has been carried out. Since a webserver represents an external interface certain information about an attack is only available on the webserver, even if the attack is aimed at a downstream system. Thus logging on a web server is mandatory.

For this requirement the following threats are relevant:
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.03-28/7.0

Req 32	Applicable retention and deletion periods must be observed for security-relevant logging data that is recorded locally.

From an IT security perspective, local storage of security-relevant logging data on a system is not mandatory. Since the local storage can be damaged in the event of system malfunctions or manipulated by a successful attacker, it can only be used to a limited extent for security-related or forensic analyses. Accordingly, it is relevant for IT security that logging data is forwarded to a separate log server.

Local storage can nevertheless take place; for example, if local storage is initially indispensable when generating the logging data due to technical processes or if there are justified operational interests in also keeping logging data available locally.

The following basic rules must be taken into account when storing logging data locally:

- Security-related logging data must be retained for a period of 90 days.
  (*This requirement only applies if no additional forwarding to a separate log server is implemented on the system and the logging data is therefore only recorded locally.*)
- After 90 days, stored logging data must be deleted immediately.

Deviances
Different retention periods and deletion periods may exist due to legal or regulatory requirements (especially in connection with personal data) or may be defined by contractual agreements. In these cases, the applicable periods must be agreed individually with a Project Security Manager (PSM) / Data Privacy Advisor (DPA) or are specified by them.

Motivation: Logging data is an immensely important IT security tool for preventing, detecting and clearing up system faults, security and data privacy incidents. On the other hand, the recording of logging data, like any other data processing, is also subject to legal and regulatory requirements. Accordingly, guidelines must be adhered to that reconcile the two.

Implementation example: Taking into account the current legal situation and applicable data privacy regulations, the following deletion periods for locally stored security-relevant logging data are implemented on an exemplary telecommunications system:

- Standard System Logs: Deletion after 90 days at the latest
- Logging of public IP addresses: Deletion (or anonymization) after 7 days at the latest
- Logging of the assignment of dynamic public IP addresses by the telecommunication solution: Deletion after 7 days at the latest
- Logging of non-billing-relevant call detail records: Deletion after 7 days at the latest
- Logging of the content of e-mail and SMS: Deletion after 24 hours at the latest
- Logging of the domain queries handled by the DNS server of the telecommunications solution: Deletion after 24 hours at the latest

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.01-34/8.0

Req 33	Security-relevant logging data must be forwarded to a separate log server immediately after it has been generated.

Logging data must be forwarded to a separate log server immediately after it has been generated. Standardized protocols such as Syslog, SNMPv3 should be preferred.

Motivation: If logging data is only stored locally, it can be manipulated by an attacker who succeeds in compromising the system in order to conceal his attack and any manipulation he has performed on the system. This is the reason why the forwarding must be done immediately after the event occurred.

For this requirement the following threats are relevant:
- Unauthorized modification of data
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.01-35/8.0

Req 34	For security-relevant logging data that is forwarded to the separate log server, compliance with the applicable retention and deletion periods must be ensured.

The following basic rules must be taken into account:

- security-related logging data must be retained for a period of 90 days on the separate log server.
- after 90 days, stored logging data must be deleted immediately on the separate log server.

Deviances

Different retention periods and deletion periods may exist due to legal or regulatory requirements (especially in connection with personal data) or may be defined by contractual agreements. In these cases, the applicable periods must be agreed individually with a Project Security Manager (PSM) / Data Privacy Advisor (DSB) or are specified by them.

Log server under the responsibility of a third party

If the selected separate log server is not within the same operational responsibility as the source system of the loggin data, it must be ensured that the responsible operator of the log server is aware of the valid parameters for the logging data to be received and that they are adhered to in accordance with the regulations mentioned here.

Motivation: Logging data is an immensely important IT security tool for preventing, detecting and clearing up system faults, security and data privacy incidents. On the other hand, the recording of logging data, like any other data processing, is also subject to legal and regulatory requirements. Accordingly, guidelines must be adhered to that reconcile the two.

Implementation example: Taking into account the current legal situation and applicable data privacy regulations, the following deletion periods for forwarded security-relevant logging data from an exemplary telecommunications system are implemented on the separate log server:

- Standard System Logs: Deletion after 90 days at the latest
- Logging of public IP addresses: Deletion (or anonymization) after 7 days at the latest
- Logging of the assignment of dynamic public IP addresses by the telecommunication solution: Deletion after 7 days at the latest
- Logging of non-billing-relevant call detail records: Deletion after 7 days at the latest
- Logging of the content of e-mail and SMS: Deletion after 24 hours at the latest
- Logging of the domain queries handled by the DNS server of the telecommunications solution: Deletion after 24 hours at the latest

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.01-36/8.0

Req 35	Security-relevant logging data must be provided to a security incident detection and response solution in near-real-time.

An acceptable detection and response solution for the purposes of this requirement must meet the following criteria:

- There is a continuous analysis and correlation of the logging data provided by connected IT/NT systems.
- The identification of threatening activities and ongoing attacks takes place on the basis of a continuously updated detection pattern database
- Integrated alerting processes trigger the initiation of countermeasures in the event of a find.

Such a solution is not the same as a log server in terms of its function. Accordingly, the provision to a detection and response solution must always be in addition to an existing forwarding to a log server. An exception exists if the log server used provides the logging data to a detection and response solution immediately after receipt. In this case, it is sufficient for the system to forward the logging data only to the log server.
The logging data must be provided to the detection and response solution within 5 minutes ("near-real-time") from the time it is generated in the system.

The specific technical interfaces and protocols to be supported for deployment are determined by the detection and response solution available in the system's operating environment as well as the technical basis of the system itself.

Motivation: IT/NT systems are constantly exposed to security threats and attacks. By means of a central analysis and the correlation of recorded system events of entire IT landscapes in almost real time, current threats and ongoing attacks can be detected even beyond system boundaries and appropriate countermeasures can be initiated promptly. The prompt delivery of logging data to the detection and response solution is essential for its effectiveness.

Implementation example: **Example 1:** A system based on a classic server collects security-relevant logging data in the operating system's local syslog or Windows Event Log. Logging data is continuously forwarded to a Security Information and Event Management (SIEM) for further analysis, intrusion detection, and alarm handling.

Example 2: An Endpoint Detection and Response (EDR) agent is running on a system. The EDR agent continuously

forwards the security-related logging data it collects on the system to the central backend of the EDR solution, where further analysis, intrusion detection, and alarm handling takes place

Example 3: Systems designed on the basis of cloud-native functions generate logging data directly from these functions using the cloud's own logging and monitoring infrastructure. In such a system, the generation of security-relevant logging data is specifically activated in the corresponding configuration options of the cloud-native functions used. The resulting logging data is continuously transferred to a SIEM (Security Information and Event Management) for further analysis, intrusion detection and alarm handling. Some cloud providers already provide some attack pattern detection in the cloud's own monitoring infrastructure and generate specific cloud alerts from it. These are also transferred to the SIEM.

Example 4: A system is based on a SaaS ("Software as a Service") application from a cloud provider. Typically, in the SaaS model, the cloud provider is responsible for all operational aspects of the application, including security management. The cloud customer itself has no influence on the underlying technical infrastructure or the operation of the application. Based on contractual agreements, recognized certificates, and documented self-disclosures from the cloud provider, it is formally verified that the cloud provider has implemented a security incident detection and response solution. Some cloud providers also generate dedicated logging data about security-relevant activities within the separate customer tenants of their SaaS application (e.g. changes to configuration settings, permission assignments or user accounts within the tenants) and make them available to cloud customers. These so-called audit logs are continuously transferred to a SIEM (Security Information and Event Management) for further analysis, attack detection and alarm handling.

For this requirement the following threats are relevant:
- Unnoticeable feasible attacks

ID: 3.01-37/8.0