Security requirement

Architecture of systems

Deutsche Telekom Group

Version	3.2
Date	Jul 1, 2023
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
	3.14	Security requirement

Version	State	Status
3.2	Jul 1, 2023	Released

Contact	Validity	Released by
Telekom Security psa.telekom.de	Jul 1, 2023 - Jun 30, 2028	Stefan Pütz, Leiter SEC-T-TST

Summary
Technical security requiremts for the architecture of IT and NT systems.

Table of Contents

1. Introduction

This 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.

The term "DTAG" in this document generally refers to "Deutsche Telekom Group".

2. Segregation of systems

The rule for the interplay between systems is to not rely on single locally implemented security measures. A base security is achieved through fundamental separations especially in the communications network.

Req 1	Systems must be separated from each other appropriately in line with their protection requirements.

The systems' need of protection results from different factors like, e.g., processed and stored data, services exposed and used applications. Similarly, systems on which personal data is processed must be protected against unwanted access or data flows from the same network or other networks by using state-of-the-art measures (such as firewalls). If a system is configured in layers, these must be appropriated separated. A critical system (i.e., system or component with high protection requirements as regards confidentiality, availability, integrity or data protection) has to be separated from other systems, also from other critical systems, at least logically. Requirements demanding a physical separation (e.g., in the case of very high worthy of protection) have to be reviewed and implemented.

Examples of network segmentation: VLAN, VxLAN, private VLAN or otherwise securely configured network segregation

Motivation: It is more likely for a less protected system to be compromised. This must not result in other systems with higher protection requirements being more easily attacked by this compromised system in the network. Breaking down the network makes it possible to establish a higher security level for systems requiring special protection without all systems overall having to be protected at a high cost.
The risk of compromise caused by other systems through the use of shared networks and resources should be minimized, where possible.

Implementation example: A critical customer management system is separated by VLANs from other systems, e.g., a webserver delivering banner ads. In addition, the customer management system contains a huge database cluster that is implemented in an own network segment to isolate it from log and statistic servers belonging to the same overall customer management system.

In a cloud, virtual network environments are available to separate systems, e.g. VPC (Virtual Private Cloud) on Amazon AWS.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-1/3.2

Req 2	Production systems must be completely separated from test and development systems.

Apart from servers, infrastructure elements such as the network and storage systems must be separated as well. A separation that is merely logical in parts is only permitted if it is not possible to bypass this logical separation and, on the other hand, it is ensured that there is no security impact on production systems when performing tests and/or development activities. A physical separation is advised. For reference systems must be decided whether these have a more productive character or being closer to a test environment.

If communication between these different system types is absolutely necessary, it can only be accomplished by employing security systems that control the entire communication. Apart from that jumphosts between these network areas should be used.

Testing activities related to security like penetration tests and network-based security scans must be possible at all times and without any impact on the production systems.

It is recommended to use clearly distinguishable IP address ranges for these different kinds of network areas.

Motivation: A sufficiently secure system status cannot be assumed in the case of test and development systems, in particular, because these are, by their nature, exposed to permanent changes. When linking system types to each other or when using the same platform, there is a risk that unauthorized parties will be able to access production systems and live data from within the test/development environment or that the stability of the production systems and thus the availability of the associated services will be put at risk. A test and development infrastructure that is completely independent from the production makes it possible to implement changes for test and development systems quickly and also during a frozen zone as they do not have an impact on the production systems. This way security updates for the production can faster be tested and accepted.

Implementation example: For an acceptance test environment, designated for security scans and penetration tests, a dedicated test environment has been chosen.
Another example is a performance test environment that is physically separated from the production, so that performance test activities do not have any negative impact on the production environment as it could be possible in the case of a shared environment, e.g., shared storage or network components.

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

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

ID: 3.14-2/3.2

Req 3	Segregations must not be bypassed.

Systems and system components must be separated with an identical effect at all points via which communication is possible. A network-based separation of systems (e.g., through VLANs, private VLANs or other layer-2 techniques) must take place in all connected network areas (e.g., production network, administration network, storage/backup network) according to the same logic. The same applies to other network technologies (e.g., Fiber Channel (FC)). Please note that it must not be possible to communicate between systems or have one system compromise another one using the management network.

Motivation: A separation with the intention to prevent other systems from being attacked following a compromise only generates genuine added value if it is executed on all interfaces in the same way.

Implementation example: From a “customer perspective”, presentation and database layer are separated on the network side. However, the administrative management interfaces would be connected in the same network and communication among systems would be possible. If the presentation layer was compromised, an attacker could access the systems of the database layer on layer-2 by circumventing a possible firewall.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-3/3.2

3. Communication

The classification of data and their protection requirements during transmission can be found in the Data Protection and Security Recommendation "Classification of Information" of Deutsche Telekom Group.

Confidentiality and integrity are two different objectives (integrity protection identifies changes to the data, encryption prevents unauthorized reading). Modern communication protocols provide both. Furthermore, an authentication of the communication partners is needed.

The following table gives an overview of the minimal requirements by encryption:

	Local transmission within DTAG owned data center across own systems, networks and lines	**Network within DTAG**	**Other, e.g., public network**
Confidential	encrypted or non-encrypted*	encrypted	encrypted
Internal	non-encrypted	non-encrypted	encrypted
Open	non-encrypted	non-encrypted	non-encrypted

*) non-encrypted only if protection is ensured by additional controls, see below

Req 4	Filter elements must be set up which ensure that only the necessary services of a system and its components are reachable.

Each system must be protected by an independent protection mechanism, e.g., a network firewall at layer-3 or above. In a virtualization environment this protection can also be done by a virtualized device or as part of the hypervisor.

Daemons might have started temporarily on a system which are not required in regular operation (e.g., through an attacker or a system update) and which should not be available at all. All used Internet Protocols (IPv4, IPv6) must be protected in the same way.

Motivation: An independent, network-based protection mechanism reduces the likelihood of the system becoming compromised.

Implementation example: Servers within a (sub-) network communicate with each other. However, incoming connections from outside this network are not required. The router, the firewall, a loadbalancer or an appropriate virtualized network element must prevent such communication attempts.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.14-4/3.2

Req 5	Possible communication paths between systems must be reduced by filter elements to the minimum needed to fulfill the purpose of the systems.

The default policy must be: deny any any. In case of an communication activation, a suitable trade-off must be found between rules for single ip addresses and rules for ip ranges covering more than one system. The use of ranges

avoids frequent changes of the ruleset.

To avoid activations for huge TCP/UDP port ranges, necessary services/protocols with dynamic port assignment should be investigated for alternatives, as far as a solution by using an appropriate firewall system with application-aware protocol support is not available. Otherwise, services might be accessible via the enabled ports which should actually be blocked.

Motivation: Communication channels provides remote access to systems. Less communication possibilities provides more security to the target systems.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-5/3.2

Req 6	The initiation of a machine-to-machine communication channel must follow the principle of "least privilege".

The initiation of a machine-to-machine communication should be done with an unprivileged user account, and not as system administrator. The login at the remote site must be done with unprivileged rights.

Motivation: Implementation of the principle least privilege.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-6/3.2

Req 7	If data with a need of protection is transmitted, the involved communication partners must be authenticated appropriately.

Data with a need of protection is in this case all information classed as “internal” or higher with regard to the protection goal of confidentiality or information with an increased need on integrity. For "confidential" classed data, an authentication based on IP addresses is nomally not sufficient. Usage of certificates is the preferred solution.

Motivation: Information with need of protection must not end up in the wrong hands.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-7/3.2

Req 8	Information classified as “confidential” must be transmitted in encrypted form.

Generally, confidential data must be transmitted encrypted, e.g. by using TLS, IPSec or SSH. An “end-to-end” encryp-

tion on the application level (e.g., through XML encryption or PGP) is to be preferred to encryption by the system.

The only exception to the encryption requirement exists in cases where the transmission is solely routed locally within a DTAG-owned data center across systems, networks and lines owned by DTAG. An example of this is a layer-2 switch to which all involved systems are connected locally. It must be ensured that only authorized individuals have access to this network.

If communication involves the interplay of such a trusted network with other networks, it is possible to use tunnel mechanisms with encryption (e.g., IPSec) to bridge non-trusted networks instead of protecting each connection individually. Such tunnels have to be considered as a part of the infrastructure (for further readings on this refer to the requirement about terminating IPSec tunnels).

Virtual network constructions such as VPNs or MPLS networks which work without encryption and only separate traffic from each other are generally not sufficient for the transmission of data classed as confidential. Additional devices can be used here which encrypt data at line level independently from any protocols that are transported over these lines.

Motivation: Encryption ensures that the data cannot be manipulated or read on its way from sender to recipient. Only authorized individuals are permitted to access this data.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-8/3.2

Req 9	Content classified as “internal” or not classed at all must be encrypted when being transmitted over unsecure or public networks (e.g., Internet or wireless networks).

The confidentiality of internal information cannot be ensured in networks that can be viewed by third parties. This also applies to networks within "Clouds", which are not operated by DTAG units.

Motivation: Internal DTAG data must be protected from third parties to view.

Implementation example: Usage of SSH, TLS and IPSec.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-9/3.2

4. Layer model

Req 10	Systems which provide information in need of protection must be divided into at least two layers which are represented by different networks.

Information in need of protection is all data classed as “internal” or higher with regard to the protection goal of confidentiality or data with a high need on integrity or availability. A layer model mostly consists of a presentation layer with direct access by the users, a layer with application servers and a third layer comprising the databases. Where this is simplified to only two layers, the application servers and the database servers form a common layer. The presentation layer has to be separated always. In some cases a loadbalancer can be considered as the presentation layer if the loadbalancer validates all input requests to the subsequent layers.

The layers correspond to individual networks, usually VLANs, which are connected through appropriate means, e.g., firewalls. In virtualized environments the separated layers can be realized by security features within the virtualization infrastructure, e.g., so-called "micro segmentation".

If access to data sources of multiple systems is required, this must take place from within an application layer.

Motivation: A layered model ensures that the user is never given direct access to layers with data that is to be protected. The aim is to render as few system components as possible visible to the user – internal structures must not be visible from the outside.

Attacks on TCP/IP as well as TLS terminate on a system of the presentation layer. Thus, the damage potential is significantly lower than if these attacks reach the application layer.

Implementation example: Databases are normally not addressed by users directly but via upstream application servers instead. This makes it possible to set up the databases in such a way that they are not directly accessible to the user.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-10/3.2

Req 11	The possible communication paths between the layers (networks) of a system must be reduced to the necessary connections through a filtering element.

This communication constraint has to take place via filter elements which have to be independent of the system components that have to be secured. Depending on the situation, firewalls, routers or loadbalancers with installed packet filters are suitable. In case of virtualized environments the security filtering mechanisms of the virtualization environment, e.g., so-called micro-segmentation, can be used.

Motivation: The use of active filter elements between the networks offers additional, network-based protection for the systems. Attacks on TCP/IP as well as TLS terminate on a system of the presentation layer. Thus, the damage potential is significantly lower than if these attacks reach the application layer.

Implementation example: If a system is divided into a presentation layer (e.g., web server) and another layer (e.g., databases) which are located in separate networks, communication from the web server to the database must only be possible via a firewall that is independent of these systems. This firewall is configured in such a way that it only allows for necessary connections to be established.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-11/3.2

Req 12	Information in need of protection must not be stored permanently in the presentation layer.

The presentation layer can be accessed directly (internally or externally) making it the first target of attacks. This is why information with need of protection (i.e., the protection requirement regarding the protection goal of confidentiality is “intern” or higher) must not be stored in this layer longer as absolutely needed.

Motivation: Storing this data in downstream systems reduces the risk of attack on this data.

Implementation example: When customers register at a web portal, the customer data to be protected must not be kept on the web server. It must be passed on to the next layer (e.g., an application server) for storing and further processing.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-12/3.2

Req 13	If systems or system components are accessible from external networks (i.e., Non-DTAG networks such as the Internet), they must be physically separated from internal systems.

All components of the externally available presentation layer have to be physically separated from internal systems. Normally, this is already done through divided infrastructures.

Non-DTAG networks also include networks of IT customers which access services in DTAG data centers – here the requirement does not apply in situations where the systems are solely operated for and on behalf of the customer (following the customer's requirements).

Motivation: IT/NT systems that can be accessed from public networks, for example, are exposed to considerably higher risk of attacks than internal systems. All requests and data forwarded to downstream systems such as application servers and databases must be validated. On the basis of this requirement, the risk of a system being compromised downstream can be significantly minimized.

Implementation example: A reverse proxy terminates HTTPS connections in the presentation layer. The data packets whose content is validated there (possibly using re-encryption) are forwarded to the target systems.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.14-13/3.2

Req 14	Connections from/to external systems (Non-DTAG) must be secured by an appropriate application layer gateway such as a webserver or reverse proxy.

Incoming network connections and internally initiated connections must be terminated in the presentation layer - TLS also.

For outgoing connections, it must be determined how the data to be transmitted must be protected according to the

protection requirements. If necessary, appropriate agreements with the recipient are to be concluded.

Motivation: First, internal network structures are hidden to outside systems, second, a proxy can filter the traffic and incoming content.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-14/3.2

5. Availability

Req 15	On top of a operating system instance only those services and applications may be operated together when they have the same administrators, data owners and have similar, low, protection requirements.

Systems (services or applications) with different protection requirements are generally separated from each other. With this in mind, on top of a operating system instance only those services and applications may be operated

- which have the same low protection requirements and
- which are operated by the same team and
- whose data are subject to a common liability.

Motivation: Mixed operation of different protection needs results in higher risks for applications with higher needs of protection, otherwise too expensive measures are in place for systems with lower needs.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-15/3.2

Req 16	If a system/system component is accessible from external networks (Non-DTAG such as the internet), only one application service may run on the corresponding operating system instance.

For example, a web server or a mail server is allowed, but not both on the same operating system instance at the same time. Multiple services of the same kind (e.g., web server) are allowed as long as they have a common, low need of protection. In this case sandboxing-techniques/containers ca be used. Special purpose loadbalancers are permitted to provide multiple services if their integrated security functions are considered as sufficient.

A mixture of internally and externally accessible services must be avoided in general.

Motivation: If the application / the system is being compromised, other services must not be involved.

Implementation example: Encapsulating of the application in a container oder small virtual machine. These virtual machines can run together with others on a common physical host.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-16/3.2

Req 17	Systems and components which are only accessed internally must use IP addresses which cannot be accessed from external networks (Non-DTAG such as the Internet).

This can be implemented in various ways:

- Use of special “private” or “unique local” IP addresses which are not routed on the Internet
- Use of corresponding routing and firewall rules when using other IP addresses

Motivation: This measure already ensures on the network level that systems are not addressable and thus not accessible by attackers.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-17/3.2

Req 18	If the system provides UDP based services, measures must be in place to compensate the missing security features of the stateless transport protocol.

Measures must be in place
- against processing spoofed IP packets as well as
- against abuse as an amplifier in an UDP-based attack.

Motivation: Defend Denial-of-Service attacks against the system and avoidance of amplification attacks based on the datagram character of UDP.

Implementation example:
- Use of a monitoring solution to early detect suspicious requests and initiate countermeasures.
- Defense measures within the application, to adapt application behavior.
- No processing of packets from spoofed IP sources by dropping such packets in the network.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-18/3.2

Req 19	System and data must be recoverable after a system outage.

According to availability needs measures have to be taken to recover a system in case of an incident. If an automatic restart is required, the system must not rely on dependencies on itself.

Installing a software update is also associated with the risk of failure. Here, a step-by-step mechanism can be selected, which is designed not to update the entire system in one go, but initially only parts of it (so-called "Canary Testing"). After a successful test run, the rest of the system is updated.

Motivation: The system and its data must be within its agreed availability.

Implementation example: Classical Backup and Recovery strategy, Snapshots of file systems or whole virtual machines, use of centrally managed storage with own backup, re-creation of systems according to templates and configuration data in configuration database, restore by automation tools, e.g. puppet / chef.

For this requirement the following threats are relevant:
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.14-19/3.2

Req 20	A backup & restore design applied to the system must ensure that backups that have been stored cannot be impaired in the event of a system compromise or system malfunction.

A system must not have permanent access to backups that have already been stored and are therefore currently in safe keeping in the sense of a backup & restore concept. Access must only be opened specifically for the purpose and for the duration of a data backup process or data recovery process and must be closed immediately after the end of the process. In addition, access should be opened in read-only mode as part of a data recovery process.

Motivation: If the system is compromised, archived backups that are permanently accessible can potentially also be reached by the attacker, who can thus change or damage them. In the worst case, a compromised system cannot be restored because backups are no longer available or their integrity can no longer be guaranteed.
A specific threat situation arises from malware, in particular so-called Crypto-Trojans, which are increasingly used not only to encrypt local file systems of an infected system, but also to encrypt all accessible file systems - including network drives, for example - and to make the data contained inaccessible.
An equivalent risk exists in the context of malfunctions in a system, which may damage accessible file systems or stored backups.

Implementation example: Implementation of a technical procedure to only temporarily open an (archive) network drive during a data backup run and to close it immediately after copying the data to be backed up.
However, this approach is not completely optimal, since the archive network drive can also be accessible to an attacker, such as a Crypto-Trojan, for the period of the data backup run and thus, at least temporarily, there is a risk for all data backups archived there. A better approach from this point of view would be to write the data to a backup drive in such a way that it cannot be changed by the writing system afterwards.
Another method would be a mechanism on the backup target server to move data backups into a read-only area after receiving them and thus protect archived backups against changes by a compromised source system.

For this requirement the following threats are relevant:
- Disruption of availability

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

ID: 3.14-20/3.2

Req 21	If the system is operated on a cloud platform, it must be prevented that the system (or the complete client/tenant with all its services and data) can be completely deleted accidentally or by unauthorized persons.

With an administration role that has the necessary permissions to delete resources and entire mandates/tenants on a cloud, it is possible to quickly and completely delete an entire system environment, either intentionally or by mistake. This usually also deletes backup drives and backups of this client.

Possible measures to prevent a total failure can be: Using a separate client for a second high-availability site, a policy that prevents deletion by a single account/role or at least a special protection of such a role if cloud resources are to be deleted.

Alternatively, a backup of data outside the cloud can also be a solution (just backing up the data separately should be sufficient, assuming that the environment itself and the software it contains can be fully installed and configured automatically from software sources outside the cloud environment).

Motivation: In contrast to classic machines and data centers, in a cloud there is the danger that complete (virtual) environments can be deprovisioned with a few mouse clicks in the GUI or a wrong command via the API. The system must therefore be protected against unintentional deletion and deliberate attacks on this scenario.

For this requirement the following threats are relevant:
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.14-21/3.2

6. Administration

This always refers to a network based login in contrast to direct console access to the hardware.

Req 22	The access for system and application administrators must be separated from the interface of the application traffic.

Administrative access may only be offered on the interface to this management network. Independent physical interfaces must be used if available or installable, due to the separate infrastructure of the network. These interfaces can still be accessible even if others are overloaded or disrupted. In individual cases, virtual or logical interfaces are sufficient. Naturally, for virtual systems only virtual interfaces can be provided.

The service that is used to login into the system (e.g., SSH or RDP) must only be linked to this interface that is intended for administrative activities. In case of systems which need administrative access on more than one interface, this has to be limited to the minimal number.

Motivation: Administrative access to systems generally takes place using high privileges. This separation is required in order to separate different kind of access and data flows from each other.

Implementation example: A webserver has one customer facing interface and one for internal backend communication. For system administration another interface is needed to provide administrative access (and only there).

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-22/3.2

Req 23	The security of workstations used for the (interactive) administration of production systems must be consistent with the protection needs of these systems.

Depending on the protection requirements of the systems to be administered, their criticality, size and general reasonableness, appropriate measures to secure the workstations must be taken to avoid compromising production systems in this way. Appropriate and proportionate measures have to be selected per system, customer or environment. Possibilities of securing workstations are:

- Use of special admin workstations completely separated and without standard office capabilities ("privileged workstation")
- Only highly potected access to the Internet, the WWW and to E-Mail
- Use of jumphosts for regulating access (possibly a logging jumphost in case of special requirements and subject to corresponding agreements)
- Use of appropriate (graphical) terminal solutions
- File transfer from/to the system only via intermediate systems with malware scanners
- Implemented security controls for the workstation, e.g. regularly installing security patches

If a system is only externally manageable (e.g., via internet) the administrative access to the system and applications must be restricted to specific static source IP addresses.

Motivation: Avoidance of compromising systems by malware or unauthorized access.

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-23/3.2

Req 24	If the system has high protection requirements, the interactive administrative access must happen via one or more dedicated jumphosts.

A jumphost provides a managed channel for access to systems. A jumphost is assigned to a small number of systems of one supplier and technology. Systems within the same application context which are operated by the same group of people, can use a common jumphost.

If access is required only by very few workplaces (<5), and should these be seen as safe and trustworthy, the value of the jumphost should be tested against the effort to implement and maintain it. If sufficient security for the access from these few workplaces is ensured, e.g. through firewall rules, the jumphost can be dispensed with in individual cases.

A jumphost must intercept the connection to the target system only in the case when the device of the accessing people is untrusted or a logging of all activity is needed.

Depending on the criticality of a system, jumphosts may be needed also for access from users.

Motivation: Ensure technically that only a small group of authorized people obtain access to these systems.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.14-24/3.2

Req 25	If a manipulation-resistant logging of privileged access is needed, it must take place on a special configured jumphost.

If manipulation-resistant logging of system administration tasks is required, a jumphost (hopping, terminal server) must be mandatory through technical restrictions for login into the target system. Users of the jumphost must not have administrative rights on this server. An appropriate logging has to be configured on the jumphost.

Motivation: This is the only way to ensure a reliable audit trail.

Implementation example: Administrative access from third parties to internal systems of DTAG normally underlies such requirements. An implementation requirement for such a jumphost is defined in the security requirement "3rd party access".

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

For this requirement the following warranty objectives are relevant:

ID: 3.14-25/3.2

7. Adherence to industry standards

Req 26	If a system processes or stores payment data of credit cards, the rules and requirements of PCI DSS must be fulfilled.

The PCI DSS (Payment Card Industry Data Security Standards) requirements and rules as well as other security standards of the payments industry must be complied with by systems that process, forward or store payment data of credit cards. This also applies to internal and external service providers who operate systems of this kind for Deutsche Telekom Group and, in doing so, process, forward or store payment data. Such service providers must sign a declaration of PCI DSS compliance.

Motivation: Implementing this requirement is important for Deutsche Telekom Group and their systems used for the processing of payment data to be compliant with PCI DSS. Otherwise the processing of this kind of data is not allowed.

ID: 3.14-26/3.2