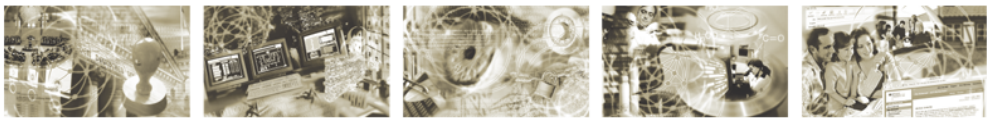
Bundesamt
für Sicherheit in der
Informationstechnik



Secure Basic Architecture for Networks Connected to the Internet (ISi-LANA)

BSI-Checklist for Internet Security (ISi-Check)

This is a work in the ISi series. A complete directory of the volumes can be found at BSI's website.

https://www.bsi.bund.de/ISi-Reihe.html

Federal Office for Information Security
ISi Project Group
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Introduction

The checklist catalogue at hand is intended primarily for administrators and security auditors who are occupied with the configuration, operation, and examination of local networks with a connection to the Internet.

1.1 Function of the Checklists

The checklists summarize the relevant recommendations of the BSI study *Secure Connection of Local Networks to the Internet* in a compact form. They serve as application assistance with which the security safeguards described in the study can be examined in detail.

The review questions are limited to the recommendations of the ISi-LANA module. General baseline security measures that are not specific to the described baseline architecture and its components are not included in the questions. Such basic recommendations can be found in the BSI Baseline Protection Catalogues [GSK2006]; there one can also find references to the corresponding checklists for baseline protection measures. The baseline protection catalogues form the foundation of ISi-Check.

The checklists are primarily intended for auditors and administrators. In-depth knowledge about IT networks and IT security is needed to use ISi-Check. The review questions do *not* replace an exact understanding of the technical and organisational relationships when a network of computers is being operated. Only an expert user is able to assess the evaluation aspects in the correct context and assess the correct and reasonable implementation of the queried recommendations in accordance with the general baseline security measures.

Thus, the primary purpose of the review questions is to give users a clear overview of the respectively necessary measures and available variations for implementation during the conception, realisation, and operation of a local network. The checklists are intended to ensure that no important aspects are forgotten.

1.2 Use of the Checklists

The ISi series is based on a comprehensive process plan that is described in the introductory document [ISi-E]. The checklists of the ISi-LANA module have their pre-assigned place in it. Before the checklists are used, the user must become acquainted with the process plan [ISi-E] and the contents of the ISi-LANA study. It is necessary to have an exact understanding of these documents in order to understand the review questions for the various evaluation aspects and apply them at the correct time.

The checklists refer to the relevant security recommendations of the study at hand without explaining them or their implementation in more detail. Users who do not understand the meaning of a review question or are not able to answer a review question with certainty can look up more in-depth information in the study. IT experts who are already well acquainted with the study should, as a rule, be able to work without referring to the study, though.

Format of the Review Questions

All review questions have been formulated so that the expected answer is "yes". Related review questions are grouped hierarchically under a higher ranking questions insofar as it makes sense to

do so. In doing so, the higher ranking question summarizes the subordinated review questions so that the affirmation of all subordinated review questions implies a "yes" to the higher raking review question.

In the case of hierarchical review questions, it up to the user whether or not she/he wishes to answer only the higher-ranking questions insofar as she/he is sufficiently well acquainted with the named evaluation aspect or the review question has little relevance in the local context. The subordinated questions serve merely as a more detailed explanation of the higher ranking evaluation criterion in the event that the user is unsure whether the concerned requirement has been sufficiently implemented. The hierarchical structure of the checklists is intended to make it easier to work through the review questions quickly and skip unimportant or obvious evaluation aspects.

Iterative Procedure

The nesting of the review questions also makes an iterative procedure possible. In doing so, the user only answers the higher ranking questions in the first step in order to get a quick overview of implementation problems. Evaluation complexes with higher ranking questions that cannot be answered with an unequivocal "yes" in the first step are prioritised in the second step and completely worked through in order based on their urgency.

Normal and High Protection Requirement

All review questions that are not labelled otherwise refer to the obligatory requirements in the case of the normal protection requirement. Naturally, these also have to be taken into account in the case of a high protection requirement. Insofar as special requirements are to be fulfilled for a high protection requirement, the label "**[High Protection Requirement]**" should precede the corresponding review question. If the question regards a certain basic security value with a high protection requirement, then the label is based on the baseline value, such as "**[High Availability]**". Users who only have a normal protection requirement can disregard the questions labelled in this manner.

Variations

Sometimes there are different choices for ways to implement a recommendation. In such cases, a higher ranking question introduces the evaluation aspect. Under it there is a review question for each of the possible implementation methods. The questions are linked to each other with an "**- or -**". Thus, in order to fulfil the higher ranking evaluation criterion, at least one of the subordinated review questions must be affirmed.

If there is a question labelled "**[High Protection Requirement]**" among the available review questions then at least one of the thus labelled variations must be affirmed in order for the higher ranking evaluation criterion to be fulfilled in the event of a High Protection Requirement.

2 Design

Pursuant to [ISi-E], a secure network architecture must be created in the design phase of the process plan. The checklists in this section scrutinize whether all recommendations for a secure basic architecture have been implemented correctly.

2.1 Internal Network (LAN)

☐ Have all components in the internal network been assigned a private IP-address?

☐ Are all IP addresses, where necessary, static configured?

- ☐ *Do all server and network switching elements in the LAN have fixed, static configured IP addresses?*
- ☐ **[High Protection Requirement]** *Do all client computers in the LAN have fixed, static configured IP addresses, and DHCP is not used?*
- ☐ **[High Protection Requirement]** *Are static assignments of MAC and IP addresses configured in the ARP tables to protect the components against ARP spoofing?*

☐ Has the LAN been segmented into suitable separate security zones?

- ☐ *Does the LAN include at least two security zones, one for the client computer, one for the server?*
- ☐ **[High Protection Requirement]** *Are security zones with High Protection Requirement hived off in separate segments?*
- ☐ *Do all systems within a security zone have a homogenous security requirement?*
- ☐ *Are the security zones separated from each other physically with a security gateway that consists of at least one packet filter?*
- ☐ **[High Protection Requirement]** *Are security zones with high protection requirement separated from other LAN segments by a three-level PAP security gateway?*
- ☐ *Has it been ensured that the separation between security zones is based on more than just logical segmentation (VLAN technology)?*

☐ If applicable, are any WLAN access points at hand separated adequately from the cable based LAN segments? This means:

- o No WLAN is used at all in the LAN? **-or-**
- o All WLAN access points are kept in their own security zone that is separated from cable-based LAN segments by a security gateway (at least one packet filter).

☐ Does the LAN have an internal server for e-mail and DNS that is only accessible to local clients?

☐ Are separate functions realised with separate components (“one service per server!")?

☐ **[High Confidentiality]** Is confidential data traffic also encrypted within the internal network?

☐ **[High Availability]** Does the internal network have a redundant design?

2.2 Security Gateway

☐ Is the structure of the security gateway appropriate for the protection requirement? This means:

- o Is the security gateway set up as three-level PAP-architecture with stateful packet filters? **-or-**
- o It concerns an uncritical IT infrastructure with a normal protection requirement at the most, and the security gateway consists of at least one stateful packet filter?

☐ Is the possibility of partial or complete elusion of the security gateway when Internet services are being used by means of other LAN outputs (such as modems) or parallel administration connection (such as an out-of-band management network) excluded?

☐ Is access from the Internet to services and applications limited to those that expressly may be offered publicly pursuant to the security policy?

☐ *Does the filtering in the security gateway occur pursuant to the whitelist principle (i.e. communication connections that are not expressly allowed are prevented)?*

☐ *Is it ensured that direct access from the Internet to the internal LAN is prevented?*

☐ *Does all allowed access from the Internet to a server terminate in a DMZ of the security gateway or at least a proxy of the ALG?*

☐ Are separate functions realised with separate components (“one service per server!")?

☐ **[High Protection Requirement]** Does the Gateway have a separate outer packet filter for the use and provision of Internet services?

☐ Is there a separate external DNS server for name resolution available for DMZ segments in which publicly accessible servers (such as web servers) have been placed?

☐ Have DNS and public services been sufficiently decoupled? This means:

- o Are DNS and services realised by means of separate servers? **-or-**
- o Were the potential disadvantages of a consolidation of DNS and services on a joint computer considered and accepted in the security policy?

☐ Are the public web services realised in the DMZ as a three-layered architecture consisting of the web server, application server, and database server? This means:

- o Are the three layers located in separate security zones that are staggered one after the other that have been separated from each other by (at least) one packet filter? **-or-**
- o Are the three layers located in separate security zones that have been separated from each other by (at least) one joint packet filter amongst each other?

☐ Is there a clear separation between the internal and external uses of public local web services?

☐ *Do accesses from the LAN to a public local web service occur through an inner web server that accesses the application server independent of the outer web server?*

☐ *Are the outer and inner web servers kept in physically separated security zones?*

☐ *Are the LAN and the inner web server separated by a three-level PAP1 security gateway?*

☐ Have all components in the security gateway been assigned a private IP-address?

☐ Are the IP addresses in the security gateway static assigned?

☐ *Do all server and network switching elements have fixed, static configured IP addresses?*

- ☐ **[High Protection Requirement]** *Are static assignments of MAC and IP addresses configured to protect the components against ARP spoofing?*

☐ Are the IP addresses of the local network hidden to the outside world?

- ☐ *Are private addresses of the services visible to the outside implemented by means of address implementation in the outer packet filter in public IP addresses (NAT)?*
- ☐ *During the address conversion at the outer packet filter, are all addresses that are to be publicly accessible pursuant to the security policy converted to the associated public address?*
- ☐ *Are all addresses that are* **not** *supposed to be publicly accessible pursuant to the security policy blocked at the security gateway?*

☐ Is all routing within the security gateway static and have all dynamic routing protocols within the security gateway been deactivated?

☐ **[High Availability]** Is the connection to the Internet sufficiently available?

- ☐ *Does the security gateway have a redundant design?*
- ☐ *Is the Internet connection set up in a corresponding high-availability manner?*

2.3 Internet Connection

☐ Does the benefit of an Internet connection outweigh the risks associated with it? This means:

- o Does the local network have a normal or at the most high protection requirement? **-or-**
- o Despite a very high protection requirement, is there an urgent need for an Internet connection and does the security policy express accept the risks in conjunction with this for lack of a better alternative?

☐ Can the Internet service provider guarantee sufficient quality of service and availability?

- ☐ *Is the required quality of service and availability described in the security policy?*
- ☐ *Is there a corresponding agreement on quality of service with the Internet service provider?*
- ☐ **[High Availability]** *Is the local network connected in a multi-legged manner to different Internet service providers or at least on independent access point of the same service provider?*

☐ **[High Availability]** Is bandwidth management used in order to use the available transmission capacity of the Internet connection optimally?

2.4 Network Management

☐ Is adequate centralized control guaranteed for all components of the network? This means:

- o Are all network switching elements and the server of the local IT infrastructure centrally remotely administered? **-or-**
- o Is this a small IT infrastructure with few components, little geographic extent, and a normal protection requirement at the most?

☐ Do the protocols used for remote administration have mechanisms for authentication, security data integrity, and encryption of the transmitted data? Are these mechanisms used throughout?

☐ Is a secure separation between payload data connections and administration connections guaranteed? This means:

- o Do all network switching elements and servers have a separate management interface by means of which they are connected in an independent management network (complete out-of-band-management)? **-or-**
- o Is the in-band management limited to the network switching elements and servers in the internal network that is connected to an independent management network through a separate management interface of the standard gateway that connects all management interfaces of the IT infrastructure (partial in-band management)?

☐ Has the management network been subdivided into suitable protective zones in order to exclude infiltration of the system administration or elusion of the security gateway through a management connection? This means:

- o Has the management network been subdivided into staggered security zones for the administration of the outer, middle, and inner IT components that have each been separated by a packet filter? **-or-**
- o Has the management network been subdivided into staggered security zones for the administration of the outer, middle, and inner IT components that are connected to a join packet filter and separated by it?

☐ **[High Protection Requirement]** Is the physical segmentation of the management network strengthened by special safeguards? This means:

- o Are high value packet filters used in the management network that also support filter functions on the application level? **-or-**
- o Are staggered filter components (packet filter, ALGs) from different manufacturers with different technologies (e.g. operating systems) used in the management network in order to reduce the risk of component-specific security vulnerabilities? **-or-**
- o Has the management network been subdivided into staggered security zones for the administration of the outer, middle, and inner IT components that are operated without a physical connection to each other as isolated management cells?

☐ Is adequate centralized control guaranteed for all administrator IDs? This means:

- o Are the administrator IDs managed in a central authentication server (e.g. RADIUS) in the management network? **-or-**
- o Is this a small IT infrastructure with few components, little geographic extent, and a normal protection requirement at the most?

☐ Is suitable central control over all log data and system registrations (traps) of the administrative components guaranteed? This means:

- o Are log data and system registrations recorded centrally in a separate management network and merged in a management server? **-or-**
- o Is this a small IT infrastructure with few components, little geographic extent, and a normal protection requirement at the most? **-or-**
- o **[High Protection Requirement]** Is this an IT infrastructure with a high protection requirement and isolated management cells, the management terminals of which are placed within eyeshot of each other?

- ☐ Are the most important performance parameters of the system components monitored continuously?
  - ☐ *Are the base performance parameters of all relevant components recorded (e.g. memory reserves, CPU load, interface utilisation?*
  - ☐ *Is there sufficient processing capacity in the management network for the transmission, assessment, and archiving of the recorded data?*
  - ☐ *Are the data assessed regularly and promptly?*
  - ☐ *Is an alarm set off without delay in the event of critical system reports?*
- ☐ Are the system clocks of all administrative components securely synchronised?
  - ☐ *Are the components operated as clients in the client-server module of the NTP?*
  - ☐ *Do NTP clients authenticate the time server by means of corresponding NTP options?*

3 Selection of Secure Components

Pursuant to [ISi-E], the realisation phase of the process plan begins with the selection of suitable components that have the security properties needed in order to implement the security concept. The checklists in this section scrutinize the suitability of the intended components. The review questions can be used as aids in the preparation of calls for tenders or as the benchmark for comparing competing products.

3.1 General Aspects

The following review questions relate to security aspects that are generally important regardless of the exact type of component.

Basic Functionality

☐ Are the components sufficiently low maintenance and easy to maintain?

☐ Do all components have the ability to deactivate unused interfaces, modules, and functions?

☐ Do all components support protocols that conform to the standard for the basic service and management functions (e.g. for DNS, NTP, SMTP, SNMP, SSH) in the current protocol versions?

☐ Do the protocols support secure cryptographic methods that conform to the standard?

- ☐ *Do the components offer authentication, securing data integrity, and encryption options that conform to the standard for the supported protocols?*
- ☐ *Is the authentication, securing data integrity, and encryption realised on the basis of cryptographically strong algorithms with sufficient key length?*

☐ Do the components save local passwords, certificates, etc. in secure, encrypted form?

Network Management and Logging

☐ Do all components support personal user and administrator IDs?

☐ Do all networking switching elements and servers support secure central network management?

- ☐ *Do all components have suitable interfaces for out-of-band remote administration with secure protocols (e.g. SSH-2, HTTPS, SNMPv3)?*
- ☐ *Can insecure protocols (e.g. Telnet, FTP) be deactivated?*
- ☐ *Can the interface for in-band administration be deactivated if necessary?*
- ☐ *Do the components support the use of a central authentication server (e.g. RADIUS)?*
- ☐ *Do the components support NTP in the client-server mode with authentication option?*
- ☐ *Do the components support syslog and event notifications (SNMP traps)?*
- ☐ *Can the access to the management accesses of the components be limited to individual origins (management computer)?*
- ☐ *Can the management access rights be limited if necessary (e.g. to read-only accesses)?*

☐ Do the components have an import/export interface for all configuration settings, preferably in a text format (e.g. XML)?

☐ Is it possible to log all changes to the configuration of the administrated components in a traceable manner?

Provider

☐ Does the provider of the IT components guarantee adequate and quick technical support of their products?

- ☐ *Does the provider guarantee long-term support for its products?*
- ☐ *Are updates and patches provided without delay after vulnerabilities become known?*
- ☐ *Does the provider give recommendations on short notice for workarounds for covering the period of time before a critical security patch becomes available?*
- ☐ *Does the provider offer customer service in German?*
- ☐ *Is customer service available at any time during normal working hours?*
- ☐ *Is the provision of replacement devices guaranteed in emergencies?*

3.2 Switches

The following review questions concern the selection of switches.

☐ Does the switch support the common spanning tree protocols (e.g. STP, RSTP, MSTP)?

☐ Can the Bridge Protocol Data Units (BPDU packets) at the terminal device be deactivated in order to refuse client computers access to spanning tree protocols?

☐ It is possible to apply terminal device ports with device address limitations?

- ☐ *Is it possible to authenticate the terminal device on the basis of its MAC address?*
- ☐ *Can the number of allowed MAC addresses per switch port be limited to one address per port?*
- ☐ *Is it possible to limit the connection of clients to all terminal device ports to one defined MAC address?*

☐ **[High Protection Requirement]** Does the switch support terminal device authentication pursuant to IEEE 802.1x?

☐ Does the switch have suitable VLAN functionality?

- ☐ *Does the switch support VLAN-standard IEEE 802.1q?*
- ☐ *Can the VLAN functionality be set separately for each port?*
- ☐ *Does the switch configuration allow differentiation between terminal device and trunk ports?*

3.3 Stateless Packet Filters

The following review questions summarize the minimum requirements for stateless packet filters.

☐ Does the packet filter support the filtering (forwarding or discarding) or data packets pursuant to the typical filter criteria for the protocols IP, ICMP, UDP, and TCP?

- ☐ *IP: Is filtering of the packet on the basis of the IP source and target address (computer address or subnetwork address) possible?*
- ☐ *Is filtering on the basis of the IP protocol number of the packet possible?*
- ☐ *Is filtering based on the ICMP message type and the ICMP code of the packet possible?*
- ☐ *Is filtering on the basis of the TCP flag of the packet possible?*
- ☐ *Is filtering on the basis of the source and target port of the packet possible for TCP and UDP packets?*

☐ Is the independent filtering of different traffic flows guaranteed?

- ☐ *Is independent filtering in the incoming and outgoing transmission directions (ingress/egress) possible?*
- ☐ *Is independent filtering possible for each device connection?*

☐ Is it absolutely clear in which sequence the defined filter rules are applied and if the first or last of the applicable rules decides on access?

☐ Can whitelisting be implemented in the components without great effort? This means:

- o Are all data packets to which none of the defined filter rules are applicable automatically discarded? **-or-**
- o Can a whitelisting strategy be realised systematically with little effort by means of suitable configuration specifications?

☐ Does the packet filter support detailed logging of all filter activities, in particular the discarded data packets?

- ☐ *Is the logging of the source and target addresses of all objectionable packets?*
- ☐ *Is the logging of the source and target ports possible?*
- ☐ *Does the logging include the date and time?*

3.4 Stateful Packet Filters

All of the review questions above for stateless packet filters apply in an analogous manner for stateful packet filters. Furthermore, the following aspects are also to be evaluated.

☐ Is it possible to occupy the ID field in the IP header with random values?

☐ Does the packet filter support the selection of random TCP sequence numbers when establishing a connection?

☐ Does the packet filter support options for the defence against fragmenting attacks?

- ☐ *Is it possible to indicate a minimum accepted fragment size?*
- ☐ *Is it possible to limit the allowed number of fragments per frame?*

☐ Does the packet filter support stateful TCP filtering?

- ☐ *Is it possible to specify an upper limit for the number of half-open TCP connections?*
- ☐ *Is it possible to discard packets with nonsensical TCP flag combinations?*
- ☐ *Is it possible to specify the allowable direction of the establishment of a TCP connection?*

☐ Does the packet filter support stateful UDP filtering?

- ☐ *Is it possible to specify rate limits for UDP?*
- ☐ *Is it possible to allow UDP traffic for a limited time only relative to the first UDP transmission (quasi the "opening of the session") between the concerned communication end points?*

☐ Does the packet filter support stateful ICMP filtering?

- ☐ *Is it possible to allow ICMP traffic for a limited time only relative to the first ICMP transmission (quasi the "opening of the session") between the concerned communication end points?*

Special Requirements for the Outer Packet Filter of the Security Gateway

☐ Does the outer packet filter of the security gateway (designated as PF1 in the basic architecture) support static address execution (NAT)?

3.5 Perimeter Router

Generally, all of the review questions for stateless packet filters apply for the perimeter router. Furthermore, the following aspects are to be evaluated.

☐ Does the perimeter router support static routing?

☐ Does the perimeter router support secure dynamic routing protocols?

- ☐ *Does the perimeter router support dynamic routing protocols that make secure authentication and security data integrity of the transmitted routing data possible?*
- ☐ **[High Confidentiality]** *Does the router support dynamic routing with encrypted routing protocols?*

☐ Is it possible to lock functions that are questionable from a security point of view at the perimeter router?

- ☐ *Can source routing be deactivated?*
- ☐ *Can Directed Broadcast [RFC 2644] be deactivated?*
- ☐ *Can the ICMP Router Discovery Protocol (IRDP) be deactivated?*
- ☐ *Can the proxy ARP function be deactivated?*

3.6 Application-Level Gateway

The following evaluation aspects are to be considered when selecting an Application Level Gateway (ALG).

☐ Can the ALG be tailored flexibly to the protocols needed by the local network?

- ☐ *Does the ALG support all protocols needed for the Internet communication (at least DNS, SMTP, HTTP, and HTTPS with certificate verification?*
- ☐ *Is it possible to retrofit security proxies for additional protocols?*
- ☐ *Is it possible to remove or lock support of protocols in the ALG that are unneeded?*
- ☐ *Is it possible to set up a TCP relay in an emergency for a protocol that is not supported?*

- ☐ *Does the ALG have a decoupling interface for any protocol in order to supplement external extensions in a modular manner?*
- ☐ *Are protocols for which there is no proxy in the ALG blocked?*

Additionally, the following protocol and application specific aspects are to be evaluated.

Review questions regarding HTTP and HTTPS Proxies

- ☐ Is it possible to exchange the browser ID of the client computer in the case of outgoing HTTP connections?
- ☐ Does the ALG have adequate filtering capabilities for HTTP traffic?
  - ☐ *Is it possible to filter request and response headers based on user-defined specifications or HTTP connections?*
  - ☐ *Can the ALG filter websites based on their Internet address (e.g. URL)?*
  - ☐ *Is it possible to filter active contents or certain MIME types?*
  - ☐ *Is it possible to filter access based on the attached cookies?*
- ☐ Is it possible to limit SSL/TLS connections in such a manner that only secure cryptographic processes and keys of a required minimum length are accepted for establishing a connection?
- ☐ Can the ALG monitor the validity of SSL/TLS certificates and deny connections in the event that the certificate is valid?
  - ☐ *Is it possible to verify the certificate chain up to the root certificate?*
  - ☐ *Is it possible to compare the requested URL with the URL identified in the certificate ("common name")?*
  - ☐ *Is it possible to check the expiration date of the certificates?*
- ☐ Can root certificates be configured flexibly in the ALG?
  - ☐ *Is it possible to retrofit one's one root certificates that are to be considered trustworthy by the ALG during the evaluation?*
  - ☐ *Is it possible to remove specific root certificates that were preconfigured by the manufacturer in order to revoke the trust for the certificate chain based on it?*

Review Questions Regarding SMTP

- ☐ Does the ALG make it possible to filter e-mail messages based on user-defined criteria?
  - ☐ *Is it possible to filter SMTP messages based on their IP address, e-mail address, or on the basis of the domain-name?*
  - ☐ *Is it possible to block data attachments of certain configurable types?*
  - ☐ *Does the ALG support grey-listing for defence against unwanted advertising e-mails?*
- ☐ Does the ALG have a decoupling interface for connecting a virus protection program or a spam filter?

Review Questions Regarding DNS

- ☐ Is the ALG able to limit DNS inquiries to certain IP addresses or IP subnetworks?

☐ Is it possible to filter DNS inquiries based on so-called recursion bits (recursion desired, RD)?

☐ Is it possible to suppress or replace the DNS version number in DNS messages?

3.7 DHCP Server

In addition to the general IT-Grundschutz requirements for servers, the following review question is to be evaluated.

☐ Can the DCHP server be configured in such a way that only DHCP clients with a registered device address are accepted?

3.8 NTP Server

In addition to the general IT-Grundschutz requirements for servers, the following review questions are to be evaluated.

☐ Does the NTP server support the required NTP operation types and options?

- ☐ *Does the server make connection of a DCF77 reception module possible?*
- ☐ *Does the server support the client-server-mode with authentication of the server?*
- ☐ *Is it possible to deactivate the broadcast mode of the NTP protocol?*

3.9 DNS Server

In addition to the general IT-Grundschutz requirements for servers, the following review questions are to be evaluated.

☐ Is it possible to limit DNS inquiries to certain sources and inquiry modes?

- ☐ *Can recursive DNS inquiries be limited to individual subnetwork addresses?*
- ☐ *Can zone transfers of the DNS server be limited to the IP addresses of authorised DNS partner servers?*
- ☐ *Can the dynamic updating of the DNS data be deactivated?*
- ☐ *Can the DNS server deny inquiries that do not have a set recursion bit (recursion desired, RD)?*

☐ Does the DNS server have options can make the spying out of the DNS more difficult?

- ☐ *Is it possible to suppress or cloak the DNS version number?*
- ☐ *Can the list-domain-function of the DNS server be deactivated?*

3.10 VPN-Box

VPN support is an optional modular extension of the security gateway. Insofar as a VPN is to be operated, the following review questions are to be evaluated.

- ☐ Can a secure, encrypted VPN (Secure VPN as opposed to a Trusted VPN) be realised with the VPN components?
  - ☐ *Do the components offer sufficiently strong cryptographic processes and sufficient key lengths?*
  - ☐ **[High Confidentiality]** *Do the components have a permit for the transmission of classified items up to and including the TOP SECRET class?*
- ☐ Do the components offer sufficient throughput for the expected amount of communication?
- ☐ Do the components make address execution (NAT) possible if needed?

4 Configuration

The checklists for the configuration are intended primarily for administrators who want to set up a secure network. The following section thus serves as a resource for auditors who wish to subject an existing network to a security audit.

4.1 General Aspects

The following review questions concern evaluation aspects that are relevant to all components regardless of the exact type of component.

Baseline Functionality

☐ Are protocol variations that conform to the standard and which are not proprietary preferred?

☐ Are the available authentication and encryption mechanisms of the used protocols and services activated?

☐ Are the authentication and encryption options limited to the selection of strong cryptographic procedures with sufficient key lengths? Is the use of weak procedures and short key lengths expressly blocked?

☐ Is the software on the components up-to-date, minimal, and restorable at any time?

- ☐ *Is the newest recommended operating system version used?*
- ☐ *Have all recommended updates and patches been installed?*
- ☐ *Have unneeded functions from the configuration been removed or at least shut down? Was using specially hardened system software variations considered?*
- ☐ *Was the software configuration updated in this manner secured so that it can be restored at any time with little effort?*

☐ Does the configuration ensure a “fail secure” response, i.e. do the components switch into a secure mode in the event of an error or restart?

☐ Do the components cloak their configuration settings to the outside?

- ☐ *Are all unneeded inquiry interfaces and information services removed or shut down?*
- ☐ *May only management connections (e.g. accesses from the management network with administrator ID) access the inquiry interface?*
- ☐ *Were the available mechanisms used in order to cloak the exact version of the used software module cloaked or hidden (e.g. suppression of version numbers in logs, replacement of information relevant to security with harmless information)?*

Network Management and Logging

☐ Have all users and administrators been assigned personal, secure IDs?

- ☐ *Have separate, personal IDs been set up for all users and administrators?*
- ☐ *Are all IDs protected by ID-specific passwords, certificates, or the like?*
- ☐ *Are secure passwords used? Is the password quality checked automatically?*

- ☐ *Are the minimum access rights configured for each ID?*

☐ Are user and administrator sessions given a time limit (e.g. screensaver with password protection, automatic logout)?

☐ Was the interface for in-band management locked for all components that are subject to out-of-band management?

☐ Are the separate management interfaces configured as dedicated management accesses to which no payload data connections can be routed?

☐ Was the remote administration limited to secure protocols and secure remote stations?

- ☐ *Has the access to management interfaces been limited to authorised management systems?*
- ☐ *Have insecure protocols (e.g. Telnet) been deactivated?*
- ☐ *Have the security options (e.g. encryption, authentication) of the used protocol been fully exploited?*

☐ Have the kind of scope of the logging in the security guideline been sensibly specified and configured pursuant to these specifications?

- ☐ *Were redundant accounting functions shut down?*
- ☐ *Are sufficient resources reserved for the collection, transmission, assessment, and archiving of log data?*
- ☐ *Are critical messages forwarded automatically without delay to the competent personnel?*
- ☐ *Is the log depth compliant with the statutory provisions on data protection?*

4.2 Switches

The following evaluation aspects are to be taken into account for the switch configuration.

☐ Has the local network been realised as a so-called switched Ethernet?

☐ Have all unused switch ports been blocked?

☐ Have the allowed clients per terminal device port been sufficiently limited by means of restrictive configuration specifications? This means:

- o Has the allowed terminal device address been limited to one MAC address per terminal device port? **-or-**
- o Has a fixed MAC address been specified for each terminal device port? **-or-**
- o Is the terminal device authenticated at each terminal device port on the basis of its MAC address? **-or-**
- o **[High Protection Requirement]** Is the terminal device authenticated at the switch pursuant to IEEE802 by means of user ID and password or client certificate?

☐ Are spanning tree protocols protected against manipulation?

- ☐ *Are spanning tree protocols deactivated at all terminal device ports (i.e. are BPDU packets discarded at the terminal device ports)?*
- ☐ *Are spanning tree protocols limited to the switch ports necessary for STP?*

☐ Are network attacks by means of VLAN manipulations prevented? This means:

- o Has the VLAN function of the switches (Standard IEEE802.1q) been deactivated? **-or-**
- o Have all terminal device ports been statically assigned to fixed VLAN?

☐ Are all available device-specific mechanisms for defence against DHCP manipulations activated (e.g. “DHCP snooping” options in the IOS operating system)?

4.3 Stateless Packet Filters

In the baseline architecture, components that function in a stateless manner are stipulated for the packet filters PF3 to PF5 and PF7 to PF10. The following evaluation criteria apply to these packet filters.

☐ Have all filter regulations been formulated pursuant to the whitelist principle ("anything that is not expressly allowed is discarded”)?

☐ Are ICMP messages to all payload data ports blocked except for those exceptions expressly included in the security concept?

☐ Are ICMP messages to the packet filters of the management network (PF7 to PF10) blocked or at least limited pursuant to the study to the recommended ICMP message codes and types?

☐ **[High Availability]** Do the packet filters have a redundant design?

☐ **[High Availability]** Are the redundant packet filters combined into a “virtual packet filter” by means of a VRRP?

☐ Is the access to the VRRP interface restricted to the necessary amount and the required group of users? This means:

- o Has the VRRP interface been deactivated? **-or-**
- o Has the access to the VRRP interface been limited by access lists to the authorised addresses (members of the redundancy group)? **-or-**
- o **[High Protection Requirement]** Is the participation in the VRRP protocol limited by the secure authentication of the members of the redundancy group?

☐ In the event of a restart or an error, does the packet filter switch into a secure mode in which it does not loosen the filter rules, but rather, at the most, makes them stricter?

- ☐ *Does the active configuration setting (running configuration) correspond to the configuration saved in the device for the restart (startup configuration)?*
- ☐ *Is it ensured that the filter blocks the communication in case of an error (instead of authorising in an uncontrolled manner)?*

4.4 Stateful Packet Filters

In the baseline architecture, components that work in stateful mode are stipulated for the packet filters PF1, PF2, and PF6. All of the review questions above for stateless packet filters apply in an analogous manner for these packet filters. These additional review questions are to be examined, too.

☐ Are the packet filters configured in such a way that they issue random Initial Sequence Numbers (ISNs) for TCP connections?

☐ Is the ID field in the IP header overwritten with random values?

☐ Is the integrity evaluation for data packets (evaluation of the checksums in the packet header) evaluated?

☐ Is IP fragmenting in the configuration limited by suitable restrictions?

- ☐ *Has a sensible minimum fragment size been defined?*
- ☐ *Has a sensible upper limit for the number of fragments per frame been defined?*

☐ Are TCP connections filtered restrictively?

- ☐ *Have sensible upper limits for the number of half-open TCP connection been defined?*
- ☐ *Are the operations for discarding nonsensical TCP flag combinations (e.g. SYN-FIN, SYN-RST) activated?*
- ☐ *Is the allowable direction of the establishment of the connection specified - where sensible?*

☐ Are stateful filter rules defined for UDP (e.g. rate limits, limited time frame after initiation of the data exchange, and stipulated direction of contact)?

☐ Is ICMP traffic filtered effectively for *payload data connections*?

- o Is ICMP traffic blocked for payload data connections? **-or-**
- o Has ICMP traffic on payload data connections been regimented in well-founded exceptions by means of stateful filter rules (e.g. by means of limited timeframes after initiation of the exchange of data)?

☐ Has ICMP traffic *in* the management *network* been regimented by means of stateful filter rules (e.g. by means of limited timeframes after initiation of the exchange of data)?

Special Requirements for the Outer Packet Filter of the Security Gateway (PF1)

☐ Does the outer packet filter (PF1) of the security gateway make a static address execution (NAT) for all computers visible in the Internet?

☐ Have all internal components that are not supposed to be directly reachable in the Internet been excepted from the address execution?

4.5 Perimeter Router

Generally, the review questions for stateless packet filters apply for the perimeter router. Furthermore, the following questions are to be evaluated.

☐ Does the perimeter router use secure routing strategies? This means:

- o Has dynamic routing been deactivated on the perimeter router? **-or-**
- o Is dynamic routing limited to secure routing protocols that guarantee security data integrity and authentication of the communication connections?

☐ **[High Confidentiality]** Are the used dynamic routing protocols encrypted?

☐ Is ICMP traffic at the Internet interface of the perimeter router filtered effectively? This means:

- o Is ICMP traffic blocked completely? **-or-**
- o Are the well-founded exceptions limited to the ICMP traffic recommended in the study?

- ☐ Are the ICMP message types that are questionable from a security perspective blocked at the Internet interface of the perimeter router?
  - ☐ *Is ICMP redirect blocked?*
  - ☐ *Is ICMP mask reply blocked?*
- ☐ Are functions at the perimeter router that are questionable with regard to security aspects blocked?
  - ☐ *Is source routing deactivated?*
  - ☐ *Has Directed Broadcast been deactivated?*
  - ☐ *Has the ICMP Router Discovery Protocol (IRDP) been deactivated?*
  - ☐ *Has the proxy ARP function been deactivated?*
- ☐ Have anti-spoofing filter rules pursuant to the recommendations [RFC 1918, RFC 2827, RFC 3330] been configured on the router?
- ☐ Does the perimeter router switch into a secure operating mode after a restart or the appearance of an error?
  - ☐ *Does the active configuration setting (running configuration) correspond to the configuration saved in the device for the restart (startup configuration)?*
  - ☐ *Is it ensured that the router blocks the communication in case of an error (instead of authorising connections in an uncontrolled manner)?*

4.6 Application Level Gateway

The configuration of the ALG is to be evaluated using the following general and protocol-specific review questions.

- ☐ Are only those protocols allowed in the ALG that are allowable and desired pursuant to the Security Policy?
  - ☐ *Are all those communication relationships blocked that are not expressly allowed (whitelist principle)?*
  - ☐ *Is unchecked, blind forwarding prevented?*
- ☐ Has a security proxy been set up for all allowed protocols?
- ☐ Are encrypted connections in the ALG sufficiently controlled? This means:
  - o Are all encrypted protocols in the ALG opened for control purposes and forwarded with re-encryption as needed after the evaluation. **-or-**
  - o Is the unchecked, encrypted forwarding of protocols limited to well-founded exceptions, and are these limited to trustworthy communication partners?
- ☐ Does the ALG use the mechanisms available in the protocols in order to monitor the integrity of the data packets?
- ☐ Does the ALG ensure that the connections between the internal network and the Internet are principally initiated from the inside, and does it deny direct connection attempts that are initiated from outside to internal computers.

☐ In the event of a restart or an error, does the ALG with its proxies switch into a secure mode in which it does not loosen the filter rules, but rather, at the most, makes them stricter?

- ☐ *Does the active configuration setting (running configuration) correspond to the configuration saved in the device for the restart (startup configuration)?*
- ☐ *Is it ensured that the filter blocks the communication in case of an error (instead of authorising in an uncontrolled manner)?*

Review questions regarding HTTP and HTTPS

☐ Is undesired information removed from the request or response headers?

☐ Is the browser ID of the web client suppressed or replaced with harmless information for inquiries into the Internet.

☐ Does the ALG limit the web access to pages that are classified as allowable in the security policy?

- ☐ *Are undesired MIME types blocked?*
- ☐ *Are undesired active contents blocked?*
- ☐ *Are URLs that are classified as questionable in the security policy blocked?*
- ☐ *Are unrequested cookies blocked?*

☐ Does the ALG limit encrypted access to HTTPS connections with valid certificates that are allowed by the security policy?

- ☐ *Were all pre-configured root certifications that are not compatible with the specifications of the local Security Policy removed from the ALG configuration?*
- ☐ *Does the ALG check the certificate chain up to the root certificate and accept only those certificates with root certificates that are trustworthy pursuant to the Security Policy?*
- ☐ *Are all HTTPS connections in the ALG for which the expiry date of the certificate has been reached or exceeded discarded?*

☐ Is there a comparison between the requested URL and the common name in the certificate in the case of HTTPS requests in the ALG? Are data transmissions denied in the case nonconformity?

☐ Does the ALG limit HTTPS connections in such a manner so that only encryption procedures with adequate key lengths are possible (e.g. no SSLv2, not 40-bit keys)?

Review Questions Regarding SMTP

☐ Are all incoming e-mails checked for undesired contents before being delivered to the recipient?

- ☐ *Is each e-mail checked for malware by anti-virus software?*
- ☐ *Do all e-mails go through a spam filter?*
- ☐ *Are all prohibited file attachments in e-mails filtered pursuant to the security policy (i.e. removed, denied, or quarantined)?*

☐ Does the ALG check the addresses of the sender and the addressee of all e-mails for plausibility?

- ☐ *Are incoming e-mails with recipients not in the domains of the local network denied?*
- ☐ *Are outgoing e-mails with senders not in the domains of the local network blocked?*

Review Questions Regarding DNS

☐ Is the DNS secured against spying, hacking, and DoS attacks?

- ☐ *Are DNS inquires from the Internet that do not refer to locally managed zones (so-called recursive inquiries) denied by the ALG or answered with a reference to a competent DNS server?*
- ☐ *Is it ensured that only those DNS inquiries are accepted for which recursion bit (recursion desired, RD) has been set?*
- ☐ *In the case of DNS messages, is the version number of the DNS proxy suppressed or replaced with a harmless value?*

4.7 DHCP Server

The baseline configuration of the DHCP server is to be checked with the following service-specific review questions.

☐ Is access to the DHCP server limited to clients with previously registered MAC addresses?

☐ Are all allowable MAC addresses administered centrally?

4.8 NTP Server

The baseline configuration of the NTP server is to be checked with the following service-specific review questions?

☐ Does the NTP server provide for its clients in the client server mode of the NTP?

☐ Has the broadcast mode of the NTP been deactivated?

☐ Are the NTP messages of the server authenticated?

☐ Does the NTP server get its time information from a reliable source? This means:

- o Does the NTP server use a DCF77 receiver module as a reference time source? **-or-**
- o Does the NTP server get its time information from a trustworthy NTP server with authenticated NTP messages under local control?

4.9 DNS Server

The baseline configuration of the DNS server is to be checked with the following service-specific review questions.

☐ Are the DNS configuration and DNS information protected against spying?

- ☐ *Does the server suppress or cloak the DNS version number in its messages?*
- ☐ *Is the list-domain function of the server locked?*

☐ Is the access to the server limited to reliable communication partners and secure operating modes?

- ☐ *Is the authorisation for zone transfers limited to trustworthy counterparties?*

- ☐ *Is the dynamic updating of DNS data deactivated?*
- ☐ *Are DNS inquiries that do not relate to the locally administered zones (so-called recursive inquiries) limited to clients in trustworthy networks?*
- ☐ *Are recursive inquiries from the Internet either blocked or answered with a reference to another competent DNS server?*
- ☐ *Is it ensured that only those DNS inquiries are accepted for which recursion bit (recursion desired, RD) has been set?*

4.10 VPN-Box

VPN support is an optional modular extension of the security gateway. Insofar as a VPN is to be operated, the following checklist is authoritative for the VPN configuration.

- ☐ Is the VPN box protected against direct access from the Internet? This means:
  - o Is the VPN box placed in a DMZ of the security gateway? **-or-**
  - o Is the local LAN segment an uncritical small branch of a larger distributed LAN with normal protection requirement that is only connected with the main location with a VPN coupling and does without any other outside connection whatsoever?
- ☐ Is the VPN operated with sufficiently strong encryption procedures and with keys of sufficient length?
- ☐ Are local addresses for communication with an external VPN partner executed suitably outside of the one own LAN environment by means of NAT?

5 Operation

The requirements for the secure operation of the ISi-LANA Baseline Architecture are limited to general baseline protective measures that have already been covered sufficiently by the review questions in the BSI Baseline Protection Catalogue [GSK 2006]. The following review questions are to be highlighted in particular:

- ☐ Is the version of all component configurations known and available at all times?
  - ☐ *Are all changes to the configuration, updates, and patches archived without delay?*
  - ☐ *Are changes to the configuration traceable (version management, logging) and is it possible to reverse them easily if necessary?*
  - ☐ *Are configuration data available quickly even in the event of a failure of the management system (e.g. by means of offline archiving, or in emergencies, paper copies)?*
- ☐ Are all configuration settings that are relevant to security checked periodically for inner consistency and compliance with the applicable security policies?
- ☐ Are all local configuration changes compatible with the agreements made externally - such as with agreements with Internet service providers or registrars?

6 References

[GSK 2006] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge. BSI, http://www.bsi.de/gshb/, 2006

[ISi-E] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Reihe zur Internet-Sicherheit, Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise, http://www.bsi.bund.de/DE/Themen/InternetSicherheit/Uebersicht/Ablaufplan/ablaufplan_node.html

[RFC 1918] Internet Engineering Task Force (IETF): Address Allocation for Private Internets; RFC 1918, http://www.rfc.net/rfc1918.html, Februar 1996

[RFC 2644] Internet Engineering Task Force (IETF): Changing the Default for Directed Broadcasts in Routers; RFC 2644, http://www.rfc.net/rfc2644.html, August 1999

[RFC 2827] Internet Engineering Task Force (IETF): Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing; RFC 2827, http://www.rfc.net/rfc2827.html, Mai 2000

[RFC 3330] Internet Engineering Task Force (IETF): Special-Use IPv4 Addresses; RFC 3330, http://www.rfc.net/rfc3330.html, September 2002