Secure Connection of Local Networks to the Internet (ISi-LANA)
BSI-Policy for Internet Security (ISi-L)
Copying and Distribution

Please note that this work and all of its contents are copyrighted.

Copying and distribution for non-commercial purposes is allowed, in particular for the purposes of training, education, information, or internal announcement insofar as BSI's ISi series is named as the source.

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
© Bundesamt für Sicherheit in der Informationstechnik 2008
Inhaltsverzeichnis

1 Policy for the Secure Connection of Local Networks to the Internet
   1.1 Management Summary...
   1.2 Introduction and Overview
      1.2.1 Application Scenarios for Internet-Capable Local Networks
      1.2.2 Basics of Secure Network Operation
   1.3 Main Results of the Threat Analysis
   1.4 Primary Recommendations
   1.5 Summary

2 Glossary

3 Index of Keywords and Abbreviations
1 Policy for the Secure Connection of Local Networks to the Internet

The use of the internet has created possibilities that have made it nearly indispensable for business and administration. However, the internet brings with it significant dangers for the IT systems connected to it as well as the information processing systems that depend on it. The ISi-LANA module provides baseline security recommendations on the basic technologies needed for operating an internet-capable local network.

The ISi-L at hand is based primarily on the BSI Study: “Secure Connection of Local Networks to the Internet (ISi-LANA)”.

1.1 Management Summary

Should the web, e-mail, or other internet services be used externally as well as internally in a local network, then this local network has to be connected to an untrustworthy network (e.g. the internet). With this step, though, the operator of a LAN subjects his network, which was closed beforehand, to significant additional threats even before the first application has been installed. Attackers from the internet can exploit vulnerabilities of the internet protocols, services, and components at the basis, and spy on data traffic (sniffing), cause systems to respond in undesired ways (spoofing) or simply infiltrate the internal network (hacking).

The ISi-LANA study at hand provides recommendations with regard to how these risks can be countered for a normal protection requirement by means of a robust baseline architecture, suitable choice of devices, secure configuration settings, and controlled operation. Furthermore, variations for the high protection requirement will be shown. Thus, they offer support in the execution phase of the process plan suggested in [ISi-E] and help the user to conceive the network design, component purchasing, and the realisation and the operation of the network. The study primarily treats the three lower layers of the TCP/IP reference model: network access layer, internet layer, and transportation layer. The specific aspects of the individual services and applications are treated in other parts of the ISi series.

The focus of the study is the suggested baseline architecture for the normal protection requirement, which takes both secure use and the secure offering of services in the internet into account. This baseline architecture is subdivided into four zones.

- The first zone includes the internal network. It contains all client systems and all infrastructure and application servers that are needed for the local LAN operation.
- The three-layer security gateway that consists of an outer packet filter, an application level gateway in the middle, and an inner packet filter is found in the second zone. This design protects the LAN against attacks from the internet. Furthermore, the servers needed to offer services in the internet are offered here; they are secured in turn by packet filters that are located in so-called demilitarised zones.
- The third zone contains components for the internet connection. In the simplest case, it contains a single router with which an internet provider is connected to the network. In the case of higher requirements for the availability, the connection must have a redundant design.
- All management data are centrally collected and processed in the management zone. This is also the location of the central time server with which all system clocks in the network are synchronised.
In addition to a secure design, the purchasing and configuration of the used components is of particular importance. Comprehensive recommendations with regard to this are made in the study (ISi-S) “Secure Connection of Local Networks to the Internet”. Thus, all components should have a separate management interface or at least be able to be administered using encrypted protocols. It is also important that the packet filter be able to apply complex rules and standards in order to limit the possible data traffic in the best possible way and that the application level gateway only lets data pass that can be examined in the application layer.

In order to meet the requirements for as many operational scenarios as possible, the solution concept can be adjusted flexibly to the size and complexity of the LAN infrastructure, the number and kind of services to be supported, and the individual protection requirement of the data and applications in the various security zones. To do so, ISi-LANA includes various architecture and configuration variations in addition to the baseline architecture for the normal protection requirement: on the one hand variations for small, uncritical IT infrastructures that can be realised with reduced effort, and on the other hand variations that also comply with the requirements of a high protection requirement by means of additional safeguards or modular expansions.

1.2 Introduction and Overview

The internet originated as a small, largely closed network that in the beginning only networked a few research institutions. In the beginning, the connected participants could trust each other for the most part. The goal of the development was a reliable network. During the design of the basic internet technology, other security aspects such as confidentiality and integrity, though, played a subordinate role.

The opening of the network, its geographic spread across the globe, and its enormously increased importance to the economy have fundamentally changed the threat level, though. On the one hand, internet users are increasingly dependent on the availability of the internet; on the other hand, they are subject to ever increasing threats.

1.2.1 Application Scenarios for Internet-Capable Local Networks

Considering the threat, one can reasonably ask why the user of a local area network should allow a connection to the internet at all. The most important applications that the internet makes possible include:

- The provision of remote access for employees working outside of the office
  The internet offers a tightly woven network of access points that make it possible worldwide to establish a high-capacity data or voice connection to services at home with little technical effort and at moderate expense.

- Multi-location AN coupling (virtual private network), VPN
  The internet makes it possible to connect AN segments that are geographically separated into a logical network without having their own cable connection. The joint use of the packet-switching P infrastructure makes such connections quite inexpensive compared to the classic, cabled networks such as the SDN.

- Access to the global data resources in the internet (World Wide Web, WWW)
  The internet is in the process of replacing conventional reference works as the preferred source of knowledge. The search engines of the world wide web offer quick and convenient access to all kinds of information and services.
- Participation in electronic correspondence (e-mail)
  E-mail is now preferred to letters in business, government, and research for communication. E-
  mail is quicker, less formal, and able to transfer multimedia content directly from computer to
  computer.
- Exchange of data with business partners and authorities
  The internet makes it possible to create ad-hoc connections between any number of participants.
  The worldwide foundation for computer networks is based on the protocols of the TCP/IP fam-
  ily. They make universal, media-disruption free exchange of data possible between all different
  kinds of internet users.

All of these uses make it clear how much the internet has permeated business processes. Thus it has
become self-evident in many areas that the local IT infrastructure be opened to the internet.

1.2.2 Basics of Secure Network Operation

Even today, the exchange of data in the internet is still based mainly on the communication proto-
cols and services from the early days. Their security characteristics are no longer sufficient, though,
for today’s threat level. Technical and organisational precautions absolutely must be made for se-
cure operation of a local network that is connected to the internet.

Basic Network Protocols

Practically all internet communication is based on the internet protocol IP. It only provides mechan-
isms for addressing (IP addresses) and basic mechanisms for controlling the packet switching.
Based on the IP are the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)
which are in turn the basis for other protocols such as HTTP or SMTP, which are used by the vari-
ous applications. The meaning of the IP protocol family goes far beyond the transmission of files
between computers, though. Language (e.g. voice over IP) and multi-media contents (e.g. internet
TV) are increasingly being transmitted using a standardised IP infrastructure.
Another basic protocol is the Internet Control Message ICMP that provides functions for controlling
the flow of data. For example, one can check with ICMP whether another computer in the network
can be reached (ping) or through which substations the packets are forwarded to another computer.
The mentioned basic protocols do not offer any functions that ensure the confidentiality and integ-
rity of the transmitted data. For that reason, such functions must be implemented by the respective
applications in their own protocols.
The protocol version 6 (IPv6) has been available for quite some time as the successor to IP Version
4, which is still the most commonly used one. Unlike its predecessor, IPv6 provides mechanisms
for authentication and encryption with which the data transmission can be improved in a standard-
ised manner on the network layer. IPv6 is spreading very slowly, though.

Basic Services

In addition to the protocols, there are fundamental services that are critical for the operation of IP
networks. One of the most important services is the Domain Name System (DNS). It takes care of
the execution of the alphanumeric names in the corresponding IP addresses. The DNS service cre-
ates a hierarchical name space that is managed by the DNS servers. The namespace is divided into
zones. Each zone creates an independent administration area with a responsible name server (DNS
Primary). The responsible DNS primary forwards DNS information to downstream severs with a
limited validity period (Time to Live, TTL). These hierarchically arranged severs buffer the DNS
data sets. If a server cannot resolve the inquiry of a client locally, it forwards the inquiry to a higher ranking DNS server.

The DNS protocol is insecure. DNS information is transmitted openly and thus can be used in order to disturb the establishment of the connection. There are already suggestions for a cryptographic securing of the DNS communication. To be mentioned here in particular are the DNS Security Extensions (DNSSEC).

In order to guarantee the exchange of data between routers, the path that a data packet is to take from the source to the destination must be defined. This is called “routing”. In the internet, the de-facto standard for routing between various IP networks is the BGP protocol. The Border Gateway Protocol Version 4 (BGPv4) serves the exchange of information about the reachability of IP networks and autonomous systems. Among other things, this makes the reconstruction of the connection topology of the autonomous systems, the elimination of cyclical routes, the aggregation of routers, and the execution of routing strategies for an autonomous system possible.

The router and the switches also must be administrated and monitored. There are different protocols for this such as Telnet and SNMP (Simple Network Management Protocol), which, though, only partially provide mechanisms for secure authentication. Here, too, there are alternatives in the meantime that offer encryption and better authentication, such as SNMPv3, SSH (Secure Shell), SFTP (SSH File Transfer Protocol).

Another basic service in the network is the Network Time Protocol (NTP). This protocol serves the synchronisation of computer in IP networks. The protocol is based on a hierarchy of time servers; the highest ranking server uses, as a rule, an external time source (e.g. DCF77). NTP clients adjust their local clocks in phase and frequency to the synchronisation signals of the server.

Basic LAN Technologies

In the realm of local networks, the Ethernet is the prevailing technology that has largely pushed aside competing transmission technologies (e.g. FDDI, ATM, Token Ring).

Pursuant to the original functional principle of the Ethernet, users send their data packets through a joint bus medium. The bus creates so-called collision domains because there is signal overlapping (“collisions”) when several bus users send simultaneously. Such collisions are accepted. The disadvantage is that all messages within so-called collision domains can, among other things, be logged by anyone. These weaknesses can be significantly reduced, though, by means of the use of modern network switching elements and a suitable LAN architecture. So-called switched Ethernets make significantly better control of the network accesses and the logical network segmentation possible compared to classic bus networks. This offers a basis for secure network operations that can be developed further on the level of the internet layer by means of physical segmentation of the LANs into multiple partial networks. These safeguards all reduce the vulnerability of the network to attacks; they also reduce the scope of the damage in the event of a successful attack.

Basis for Secure IT Applications

Reliable basic technology forms the basis for secure operation of a local network with a connection to the internet. Because the internet and LAN technologies at their basis do not have sufficient security mechanisms, though, local networks must be designed from the beginning for secure operation in the internet, which concerns the selection, arrangement, and configuration of their IT components. Protective mechanisms on the application layer can only be secure against being bypassed by an attacker exploiting vulnerabilities in the lower protocol layers if the lower three layers of the TCP/IP reference model are secured.
1.3 Main Results of the Threat Analysis

The common basic technologies in the internet are receptive for various basic threats: Sniffing, Spoofing, Hacking, and Denial of Service.

Sniffing (Threat to Confidentiality)

Sniffing is the designation for techniques for spying on the data traffic of a computer network in an unauthorised manner and gaining illegal access to confidential information. Sniffing threatens the confidentiality of data processing. It can serve the purpose of obtaining information for additional attacks, such as spying out passwords.

A typical example of a sniffing attack is MAC flooding. In the case of this attack, the attacker over-whelms a switch with more and more MAC addresses until its address table floods and the switch goes into a failopen mode. In this mode, it sends all incoming messages to all connected user connections because the connection the memory is inadequate for an exact assignment of addresses. Thus, the attacker can read all of the data traffic that runs through this switch using his connection.

The elementary safeguard against all kinds of sniffing attacks is the encryption of all protocols and application data that are relevant to security.

The basic internet protocols (e.g. IPv4, UDP, TCP, ICMP) and the basic services (e.g. DNS, Telnet, FTP) send the data in an unencrypted manner, though. New protocol versions, such as IPv6 and SNMPv3, though, offer encrypted communication in the meantime. However, they are replacing the established, insecure protocols very slowly. There are still not enough available public-key-infrastructures that would make it convenient for internet users to establish encrypted connections with any communication partner. For that reason, sniffing will remain a serious threat to internet security for the foreseeable future.

Spoofing (Threat to Integrity/Authenticity)

Spoofing is the designation in information technology for various attempts at deception and cloak-ing one’s own identity and counterfeiting transmitted data. The goal is to undermine the integrity and authenticity of the information processing.

MAC Spoofing and ARP spoofing are typical kinds of attacks. In doing so, the attacker attempts to manipulate the assignment between the access port and the switch and the MAC address or between the IP address and the MAC address in such a manner that he can assume the identity of the third-party terminal device in the network. The consequence is that the data traffic intended for another terminal device is re-routed to the computer of the attacker. Such an attack also makes it possible to spread data using a feigned identity.

A similar attack is also possible on the application level. In the case of so-called DNS spoofing, the attacker manipulates the assignment between domain names and IP addresses, for example in order to pretend that his computer is a portal for online banking. If the attack is successful, the attacker can access bank transactions including the passwords, PINs, and TANs and attempt to use this information to plunder the accounts of others.

The basic safeguard against spoofing attacks is the use of protocols with secured integrity and the authentication of users, services, and hardware components.

At this time, the communication partners usually only identify themselves in the basic internet protocols using their device or IP addresses. This information, though, is easy to falsify and thus unsuitable for secure authentication. Only the use of strong cryptography makes it possible to reliably...
identify the author and intactness of the received data in an open network. New protocol versions increasingly use cryptographic verification codes. However, many devices still use the insecure old protocol versions as the standard setting when they are first set up.

**Hacking (Threat of Infiltration)**

In the context of information security, hacking designates attacks that attempt to overcome existing security mechanisms in order to infiltrate an IT system, expose its vulnerabilities, and even take it over in some cases. Hacking threatens the system sovereignty of the network operator.

The primary safeguard against hacking lies in minimizing the contact surface. However, it is difficult to foresee the "contact surface" of an IT system in each case because vulnerabilities can often be used in surprising ways. Recommended in any case as a precautionary safeguard is a physical segmentation of the IT infrastructure, filtering the data packets at a multi-layer security gateway, and strict access controls. Protection of the local network against internal attacks is also important: Should an attacker succeed in infiltrating the local network and undermining a computer there, then such safeguards limit the attacker’s area of action.

Sniffing and spoofing (e.g. the interception or surreptitious obtaining of passwords) are commonly used techniques for spreading and executing hacking attacks. Because the regular protocols and services in the internet offer little defence against spying and deception, they only offer little protection against intruders without additional security precautions.

**Denial of Service (Threat to Availability)**

Denial of Service (DoS) designates a condition in which the system refuses a service, and is thus no longer available. DoS attack is the general term for attacks that attempt to damage the availability of systems in an conscious manner. This can be done with wilfully created computing, savings, or communication loads in order to exploit vulnerabilities in software or hardware to crash a computer in a targeted manner.

In order to generate such loads, most such attacks are remote and coordinated from a large number of attacking computers; one speaks of distributed DoS attacks (Distributed DoS, DDoS).

One typical attack strategy is to use a broadcast to initiate an avalanche of answer messages that exceed the processing capacities of the recipient. For example, in a so-called Smurf Attack, a ICMP inquiry using the faked sender address of his victim is broadcast to many computers. All recipients answer the broadcast with an ICMP answer, and the collective amount of simultaneous answers crashes the victim’s computer. In a similar manner, a DNS server can be caused to trigger a cascade of recursive DNS inquiries in order to compromise the name resolution in the internet in a targeted manner (DNS Amplification Attack).

The internet’s method of functioning favours such overload attacks: The internet is based on packet switching. Data packets from different communication connections share the same sections of the transmission paths. Unlike the situation with a classic cabled network such as a telephone network for which an exclusive channel of communications with a fixed bandwidth is reserved for each connection, it is relatively easy for malicious broadcasters to overwhelm internet users with undesired data packets in a targeted manner.

Protection against DoS attacks is only possible in a limited way in the internet. The basic safeguard against malicious system crashes lies in operating a system in a minimal configuration with the smallest possible contact service and installing the latest patches of the system manufacturers as soon as possible in order to eliminate known vulnerabilities.
The most important protection against attempts at overwhelming is offered by adequate computing power reserves in order to resist an attack until the source of the attack can be made harmless in other way. Management of the broadband in a targeted manner can divide up the available transmission capacity in such a manner that the most important services always have a defined minimum amount of bandwidth available that cannot be taken away from them by applications with lower priority.

1.4 Primary Recommendations

The recommendations for the design, configuration, and operation of an internet-capable local network are based on the following basic principles:

- **Separation of functions**: Independent functions should be realised separately from each other (“one server - one service!”). This applies especially to functions that are relevant to security. The separation of functions reduces the complexity of the device configuration and minimizes the contact surface and the load on the individual components.

- **Minimality**: All system components - in particular the components of the security gateway and the servers that can be reached through the internet - should be configured minimally. Extraneous software should be removed and unneeded device functions should be deactivated.

- **Need to Know principle**: System components, applications, and services may only reveal that information about the LAN and its users that is absolutely necessary for orderly operation and use of the IT infrastructure. The accessible range of information ought to be tailored individually based on the role and access rights of the user.

- **Whitelisting**: All filter rules in the packet filters and proxies ought to be formulated in such a way that inquiries that are not expressly allowed are automatically denied.

- **Limitation of the connection establishment**: Connections may not be established from the internet into the internal network unless the service would not otherwise work (e.g. e-mail).

- **Currency**: The used operating system and application software should always be kept as up to date as possible. Available patches ought to be installed without delay.

The Baseline Architecture depicted in Figure 1.1 consisting of an internal network, an upstream Security Gateway that limits all interaction between the internet and the internal network to the necessary minimum, and the actual internet connection arises from these principles.
ISi-L - Secure Connection of Local Networks to the Internet

Recommendations for the Secure Structure of the Internal Network

The basis for secure internet use is a local network that is also resilient against internal attacks. A secure local network limits the opportunities for misuse by an external attacker who succeeded in breaking through the outer protective barriers and infiltrating internal components. The defence against internal attacks also helps prevent internal users from misusing the network as a platform for internet attacks on other IT systems.

To make this possible, the baseline architecture for the internal network is characterised by the principle of strict physical segmentation. Internal parts of the network with different if possibly equally high protection requirement (so-called security zones) are separated from each other by a security gateway. An internal security gateway consists of at least one packet filter. A purely logical “segmentation” by means of VLAN technology is not sufficient for securely separating security zones.

Thus, every non-trivial internal network is subdivided into at least two security ones, a client segment for the work station computer, and a server segment for the basic services for support of network operation. Additional segments can be augmented in order to shield data and applications with high protection requirement (e.g. personal data) from the rest of the IT infrastructure.

Data and applications that are also to be accessible from the internet may not be made available in the internal network on servers. They must be stored on external servers that are located in a so-called demilitarised zone (DMZ) of the security gateway and be accessible neither from the internet nor the local network.

Recommendations for a Secure Connection to the Internet

At the core, the solution concept for a secure connection of a local network to the internet lies in controlling the exchange of data between the internet and the local network in a three-step security gateway. This security gateway consists of an outer packet filter, an application level gateway in the middle, and an inner packet filter (PAP-structure).
The PAP- security gateway may not be circumvented; every exchange of data between the internet and the internal network must pass through the gateway. In doing so, the security gateway limited incoming and outgoing data traffic to the expressly desired protocols and services.

In order to make complete control possible, encrypted connections may not tunnel through the security gateway without being checked. The examination requires decryption and, as the case may be, re-encryption of such connections in the security gateway. Encrypted communication with select communication partners can only be passed through the security gateway without being controlled if end-to-end encryption is absolutely indispensable. Such exceptions must be expressly documented and founded in the security concept, though. In this case, additional security safeguards must then be executed on the internal client.

In the case of an internet connection, one must differentiate between two directions of communication, the use of internet services and the offering of one’s own services in the internet. Whereas the communication connection during use of the service is conducted via the three layers of the PAP gateway, external accesses to the offered internet services terminate at a server in a DMZ of the security gateway in order to protect the internal network from direct access. For their part, the upstream DMZ servers can revert to computers in downstream security zones of the DMZ if needed in order to provide services.

Figure 1.1 shows on overview of the baseline architecture for the normal protection requirement. As an example for other internet services, a web application server (WWW AS) is operated here in a hierarchically nested DMZ. The application server can be reached both from within (through the internal webservice "WWW int.") and also through the internet (through the external webservice "WWW" in the DMZ). The data in the web application are on a database server (WWW DB) that is placed in a separate security zone and administers the application data from external and internal users. Internal and external webservers function to a certain degree as service and user group-specific proxies for the web application server.

Based on the baseline architecture depicted in figure 1.1, there are numerous options for realisation, for example consolidating servers or packet filters which offer somewhat weaker protection that may also be acceptable under some circumstances with less expensive hardware. The residual risks associated with this approach must be borne consciously, though. For higher protection requirements, additional recommendations must be executed, such as redundancy safeguards. A detailed discussion can be found in the associated ISi-S.

An important security characteristic of the baseline architecture is the use of private addresses. In the entire internal network including the security gateways, private IP addresses are provided that cannot be routed in the internet. An address execution (NAT) of the externally visible, public IP addresses to internal, private IP addresses hides the internal structure of the network to the outside and thereby prevents internal computers from being attacked directly from the internet.

**Recommendations for Secure Network Management**

The relevant components of the baseline architecture - router, packet filter, security proxies and sever - must be monitored and administered continuously. For security reasons, only encrypted network management protocols should be used for this purpose. Because for security reasons encrypted connections cannot pass through the security gateway without being checked, though, it is recommended that the entire management data traffic be bundled in a separate security zone (out-of-band management).

Figure 1.2 shows the recommended baseline architecture for the network management. All management protocols (e.g. SNMP, SSH, syslog) are processed through a separate management interface of the components that is connected to a central management station through a separate network. The
operating system of a component often makes it possible to completely decouple the payload data interface from the management interfaces.

At the same time, the management station serves to synchronize all system components by means of the Network Time Protocol (NTP). A DCF77-receiver module serves as a reference time source that is independent of IT.

The baseline architecture stipulates that the management zone is to be subdivided into separate subsegments by packet filters. In this case, too, simplified variations with reduced hardware and increased residual risk are thinkable. It can be sensible for application scenarios with high protection requirement to do without a consolidation of the management segments in a central management station and, instead, to provided physically separated management stations for each sub-segment. Such a decentralised solution has specific advantages, but also has a number of security disadvantages that must be given careful consideration.

**Figure 1.2: Baseline architecture with management and monitoring module**

### 1.5 Summary

ISi-LANA treats the basics of the secure LAN operation with an internet connection, and thus primarily addresses the lower three protocol layers of the TCP/IP reference model: the network access layer, internet layer, and transportation layer. If the user follows the recommendations and applies them to expanded network architectures in an analogous way, then he has done all that is necessary to fulfil even high protection requirements with regard to the lower three layers of the TCP/IP reference model.
Naturally, security aspects of the application layer require an application-specific examination and, for that reason, go beyond the basics treated here. Such in-depth examinations are the subject of the specialised modules of the ISi series that go into detail about the application-specific peculiarities for the use of certain security technologies and commonly used internet services. Protective measures on the application layer can only be successful, though, if they cannot be subverted by attacks on the layers that are below them. With its recommendations for the secure use of the basic technologies, the ISi-LANA module creates the necessary basis for an integrated security concept.
2 Glossary

Application Layer
The application layer is the top layer in the CP/P reference model. It consists of all protocols processed by application programs, e.g. browsers or email clients, and used to exchange application-specific data. Examples of protocols in the application layer include the Hypertext Transfer Protocol (HTTP) or the imple Mail Transfer Protocol (MTP).

Applied Threat
An applied threat is a basic threat which has a direct effect on an object as the result of vulnerability. A threat therefore only becomes an applied threat for an object if the object has a vulnerability. According to the above definition it can be ascertained that all users are principally exposed to a basic threat by computer viruses on the Internet. The computer of a user who downloads a file infected with a virus is subject to an applied threat of being infected with this computer virus if this user’s computer is susceptible to this type of computer virus. In contrast, the downloading of malicious software is not an applied threat for users who use effective virus protection programs, a configuration that prevents computer viruses from executing, or an operating system that is not able to execute the virus code.

Attack
An attack is a deliberate form of threat. More precisely, an attack is an undesired or unauthorised action executed with the goal of gaining an advantage or causing damage to third parties. Attackers can also act on the behalf of third parties who wish to gain an advantage through the attack.

Authentication
Authentication is understood to be the presentation of verification that a communication partner is actually the person he or she claims to be.
**Authenticity**
The term authenticity refers to the attribute which ensures that a communication partner is actually the one he or she claims to be. When information is authentic, it is ensured that it was created by the stated source. The term is not only used when checking the identity of people, but also when verifying IT components or applications.

**Availability**
The availability of services, IT system functions, IT applications, IT networks, or even of information is guaranteed when they are available at all times for use as desired by the users. Availability is a basic value of IT security.

**Client**
The term client refers to software or hardware which is able to make use of certain services provided by a server. The term client is often used to refer to a workstation computer that accesses data and programs available on a server in a network.

**Confidentiality**
Confidentiality means protection against the unauthorised disclosure of information. Confidential data and information should only be accessible to those authorised using the allowed access methods. Confidentiality is a basic value of IT security.

**Cryptography**
A field in mathematics that deals with methods for protecting information (i.e. with the confidentiality, integrity, and authenticity of data, among other things).

**DDoS (Distributed Denial of service)**
A coordinated DoS attack on the availability of IT using a larger number of attacking systems.

**DMZ (Demilitarised Zone)**
A DMZ is an intermediate network which is located between the Intranet and the Internet, but which is not included in either network. It represents a network that is less secure than the internal network to be protected but which is more accessible from an outside network. A DMZ is used to create an additional security area for services (e.g. for email or the Web) or to create proxies that can be used by external networks but which may not be placed in the internal network for security reasons.

**DNS (Domain Name System)**
The domain name system converts alphanumerical address names (e.g. www.bsi.bund.de) into numerical addresses (e.g. 194.95.177.86). DNS can also translate addresses in the other direction. Alphanumeric names of computers are easier for users to remember and enter. However, since IPv4 and IPv6 require addresses in numerical form, the addresses must be translated by the DNS.

**DoS (Denial of Service)**
Attacks with the goal of impairing the availability of IT.
Encryption
Encryption (encipherment) transforms a plain text in accordance with an item of additional information (known as the key) into a corresponding secret text (cipher text or enciphered text), which should not be decryptable for anyone not in possession of the key. The reverse conversion - re-claiming the plain text from the cipher text - is known as decryption or decipherment.

**FTP (File Transfer Protocol)**
The file transfer protocol consists of easy to use functions for exchanging files between two computers.

**Hacking**
In the context of information security, hacking refers to attacks conducted with the goal of overcoming existing security mechanisms in order to penetrate an IT system, discover any weaknesses in the system, and possibly even take over the system in cases where the hacker is unethical.

**HTTP (Hypertext Transfer Protocol)**
The hypertext transfer protocol is used for the transmission of data, usually in the form of web pages, between an HTTP server and an HTTP client such as a browser, for example. A unique name is associated with the data using uniform resource locators (URLs). URLs are usually specified in the form "protocol://computer/path/file". "Protocol" in this case stands for a protocol in the application layer, "computer" for the name or address of the server, and the "path/file" specifies the exact location of the file on the server. An example of a URL is http://www.bsi.bund.de/topics/itgrundschoetz/index.htm.

**ICMP (Internet Control Message Protocol)**
The internet control message protocol transports error and diagnostic information for IPv4, and in the new version for IPv6 as well. It is used internally by TCP, UDP, and both IP protocols. It is used in this case when data packets cannot be delivered, a gateway reroutes data traffic over a shorter route, or a gateway does not have enough buffer capacity for the data to be processed.

**IDS (Intrusion Detection System)**
An intrusion detection system is a system for detecting attacks on a computer system or in a computer network.

**Information Security**
The goal of information security is to protect information. This information might be printed on paper, kept on computers or stored in people's minds. IT security primarily concerns protecting and processing information that is stored electronically. The term "information security" is more comprehensive than the term “IT security” and is therefore being used more and more often.
Integrity
Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is used in connection with the term "data", it expresses that the data are complete and unchanged. In information technology terms this is, however, used somewhat more widely, also for the term "information". The term "information" is used for data that, depending on the context, can be associated with certain attributes such as the author or time and date of creation. Loss of the integrity of information can therefore mean that these have been changed without authorisation, the information regarding the originator has been tampered with or that the date of compilation has been manipulated. Integrity is a basic value of IT security.

IP (Internet Protocol)
Connectionless protocol in the Internet layer of the TCP/IP reference model. Among other information, an IP header in IPv4 contains two 32-bit numbers (IP addresses), one for the destination computer and one for the source computer.

IPv4 (Internet Protocol Version 4)
Version 4 of the Internet protocol is a connectionless protocol in the network layer and allows two computers to exchange data without having to establish a connection. IPv4 does not require the underlying network to perform error detection. Furthermore, it does not provide any reliability or flow control mechanisms. IPv4 places the responsibility for most of these problems on the next highest layer (the transport layer).

IPv6 (Internet Protocol version 6)
Version 6 of the Internet protocol is the follow-up version to IPv4 and is intended as a replacement for IPv4 because, among other things, it greatly increases the number of available computer addresses and contains safeguards to protect the transmitted data against losses of confidentiality, integrity, and authenticity. The security measures are collectively referred to using the term "IPSec". IPSec defines security services that are realised using two additional headers, the "IP authentication header" (AH) and the "IP Encapsulating Security Payload" (ESP) header. Various cryptographic algorithms can be embedded with the help of the headers. IPSec allows the header to be integrated in IPv4 datagrams as well as in IPv6 datagrams. AH and ESP headers can appear individually or together in an IP datagram. The security mechanisms protect IPv4/IPv6 and the overlying protocols.

NAT (Network Address Translation)
Network Address Translation (NAT) refers to a method for automatically and transparently replacing address information in data packets. NAT methods are normally used on routers and security gateways, especially to utilise the restricted IPv4 address space as efficiently as possible and to hide local IP addresses from public networks.

Operating System
The operating system is a control program that allows a computer to be used. The user can manage files, monitor connected devices (e.g. printers and hard disks), or start programs with it. Windows, Linux, and MacOS are examples of popular operating systems.
Packet Filter
Packet filters are IT systems with special software that filters the incoming and outgoing data traffic based on special rules. The task of a packet filter is to forward or reject data packets based on the information in the header data in the IP and transport layers (e.g. the source and destination address, port number, or TCP flags). The contents of the packet are ignored in this case.

Password
A secret code word that protects data, computers, or programs, among other things, against unauthorised access.

Patch
A patch is a small program that eliminates software errors such as security gaps in applications or operating systems.

Protection Requirements
The protection requirement describes which protection is adequate and appropriate to protect the processed information and the employed information technology.

Protocol
Description (specification) of the data format used for communication between electronic devices.

Proxy
A proxy is a type of representative in networks. It accepts data from an interface and forwards it to another location in the network. Proxies are used to filter data flows and forward them selectively.

Residual Risk
Risk generally remaining even after implementing safeguards to protect the IT during use.

Router
A (IP) router is a switching processor that links the network at the IP level and decides on which route to use based on information in the IP protocol layer. Routers separate networks in the network access layer and therefore form the boundaries of the broadcast domain in an Ethernet.

Security Concept
The designed security requirements are systematically laid down in a security concept, and the procedure for their implementation is described in safeguards.

Security Gateway
A security gateway (often also called a firewall) guarantees secure connection of IP networks by restricting the technically possible communication to those types of communication that are approved in an IT security policy. In this case, security when connecting networks primarily means that only desired accesses or data streams between different networks are permitted and that the data transmitted is checked. A security gateway for normal protection requirements generally consists of several different filter components connected in series. There is a difference in this case between a packet filter and an application level gateway (ALG).
Security Policy
In a security policy, the protection goals and general security safeguards are formulated as official requirements of a company or government agency. Detailed security safeguards are contained in a more comprehensive security concept.

Server
A server is either software or hardware which offers certain services to others (namely clients). Typically this term refers to a computer which makes its hardware and software resources accessible to other computers in a network. Examples of servers include application, data, web, or email servers.

Service Provider
Providers of telecommunication or media services. Whether or not the services are offered commercially is not a prerequisite for classification as a service provider.

SMTP (Simple Mail Transfer Protocol)
The Simple Mail Transfer Protocol specifies how emails should be transmitted between servers. SMTP can also be used to transport emails from the email client to the server.

Sniffing
Sniffing refers to technologies used to read the data traffic in a data network without authorisation in order to gain illegal access to confidential information.

Spoofing
In information technology, spoofing refers to the various attempts at deception in order to conceal the user's identity and to falsify the data transmitted. The goal of spoofing is to undermine the integrity and authenticity of the information processing system.

Switch
A switch is a network component used to connect several network segments together in a local network.

TCP (Transmission Control Protocol)
Connection-oriented protocol in the transport layer in the TCP/IP reference model that is based on IP.

Threat
A threat, in general terms, is a situation or event that could result in damage. The damage is related to a concrete value such as financial assets, knowledge, objects or health. When used in the field of information technology, a threat is a situation or event that can threaten the availability, integrity, or confidentiality of information, which in turn can result in damage to the owner of the information.
Transport Layer
The transport layer in the TCP/IP reference model is the layer above the Internet layer. It is assigned the task of transporting data from the source to the destination reliably and independently from the actual physical network. The main protocols in the transport layer are the TCP and UDP protocols.

UDP (User Datagram Protocol)
The user datagram protocol is a connectionless protocol in the transport layer of the TCP/IP reference model. In contrast to TCP, it does not provide for any transport acknowledge messages or other security mechanisms for ensuring the correctness of the transmission. As in TCP, the header contains two port numbers that are associated with services in the application layer but which are independent of the port numbers used by TCP. It takes less time to process a UDP data packet than it does to process a TCP data packet. However, the shorter processing time comes in conjunction with several disadvantages such as the higher probability of losing packets, for example.

VLAN (Virtual Local Area Network)
Virtual local networks (Virtual LANs, VLANs) are used to logically structure networks. In a VLAN, a logical network structure is formed in a physical network by connecting workstations and servers with similar functions to a virtual network.

VPN (Virtual Private Network)
A Virtual Private Network (VPN) is a network that is physically operated within another network (often the Internet), but is logically separated from this network. In VPNs, the integrity and confidentiality of data can be protected and the communication partner can be securely authenticated with the help of cryptographic methods, even when several networks or computers are connected to each other over leased lines or public networks. The term VPN is often used to refer to encrypted connections, but other methods can also be used to secure the transport channel, for example special functions available in the transport protocol used.

Vulnerability
A vulnerability can result in the manifestation of a basic threat and damage to an organisation or a system. A vulnerability in an IT system can be caused by its design, the algorithms it uses, its implementation, its configuration, or its operation, but could also be caused by the organisation itself. A vulnerability can lead to a threat becoming a reality and damaging the organisation or a system. As a result of a vulnerability an object (an organisation or a system) is susceptible to threats.
## 3 Index of Keywords and Abbreviations

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>AH (Authentication Header)</td>
<td>20</td>
</tr>
<tr>
<td>ALG (Application-Level Gateway)</td>
<td>22</td>
</tr>
<tr>
<td>application layer</td>
<td>7, 9, 16, 17, 19, 23</td>
</tr>
<tr>
<td>application layer</td>
<td>7, 9, 16, 17, 19, 23</td>
</tr>
<tr>
<td>ARP (Address Resolution Protocol)</td>
<td>10</td>
</tr>
<tr>
<td>AS (Applikation Server)</td>
<td>14</td>
</tr>
<tr>
<td>ATM (Asynchronous Transfer Mode)</td>
<td>9</td>
</tr>
<tr>
<td>Attack</td>
<td>11, 17</td>
</tr>
<tr>
<td>authentication</td>
<td>8-10, 20</td>
</tr>
<tr>
<td>authenticity</td>
<td>10, 17, 18, 20, 22</td>
</tr>
<tr>
<td>authorisation</td>
<td>20, 22</td>
</tr>
<tr>
<td>availability</td>
<td>6, 7, 11, 17, 18, 23</td>
</tr>
<tr>
<td>BGP (Border Gateway Protocol)</td>
<td>9</td>
</tr>
<tr>
<td>broadcast domain</td>
<td>21</td>
</tr>
<tr>
<td>browser</td>
<td>19</td>
</tr>
<tr>
<td>cipher text</td>
<td>19</td>
</tr>
<tr>
<td>client</td>
<td>6, 9, 13, 14, 18, 19, 22</td>
</tr>
<tr>
<td>computer virus</td>
<td>17</td>
</tr>
<tr>
<td>confidentiality</td>
<td>7, 8, 10, 18, 20, 23</td>
</tr>
<tr>
<td>cryptography</td>
<td>10</td>
</tr>
<tr>
<td>DB (Database)</td>
<td>14</td>
</tr>
<tr>
<td>DCF77</td>
<td>9, 15</td>
</tr>
<tr>
<td>DDoS (Distributed Denial of Service)</td>
<td>11, 18</td>
</tr>
<tr>
<td>DMZ</td>
<td>13, 14, 18</td>
</tr>
<tr>
<td>DNS</td>
<td>8-11, 18</td>
</tr>
<tr>
<td>DNSSEC (DNS Security Extensions)</td>
<td>9</td>
</tr>
<tr>
<td>DoS (Denial of Service)</td>
<td>10, 11, 18</td>
</tr>
<tr>
<td>E-Mail (Electronic Mail)</td>
<td>2</td>
</tr>
<tr>
<td>Encryption</td>
<td>19</td>
</tr>
<tr>
<td>ESP (Encapsulating Security Payload)</td>
<td>20</td>
</tr>
<tr>
<td>Ethernet</td>
<td>9, 21</td>
</tr>
<tr>
<td>FDDI (Fiber Distributed Data Interface)</td>
<td>9</td>
</tr>
<tr>
<td>FTP (File Transfer Protocol)</td>
<td>9, 10, 19</td>
</tr>
<tr>
<td>hacking</td>
<td>6, 10, 11, 19</td>
</tr>
<tr>
<td>hardware</td>
<td>10, 11, 14, 15, 18, 22</td>
</tr>
<tr>
<td>HTTP (Hypertext Transfer Protocol)</td>
<td>8, 17, 19</td>
</tr>
<tr>
<td>Hypertext</td>
<td>17, 19</td>
</tr>
<tr>
<td>ICMP (Internet Control Message Protocol)</td>
<td>8, 10, 11, 19</td>
</tr>
<tr>
<td>IDS (Intrusion Detection System)</td>
<td>19</td>
</tr>
<tr>
<td>information security</td>
<td>11, 19</td>
</tr>
<tr>
<td>INFOSEC (Information Security)</td>
<td>2, 19</td>
</tr>
<tr>
<td>internet layer</td>
<td>6, 9, 15</td>
</tr>
<tr>
<td>intranet</td>
<td>18</td>
</tr>
<tr>
<td>IP (Internet Protocol)</td>
<td>6-10, 14, 15, 17, 19-23</td>
</tr>
<tr>
<td>IPsec (Internet Protocol Security)</td>
<td>20</td>
</tr>
<tr>
<td>IPv4 (Internet Protocol Version 4)</td>
<td>10, 18-20</td>
</tr>
<tr>
<td>IPv6 (Internet Protocol Version 6)</td>
<td>8, 10, 18-20</td>
</tr>
</tbody>
</table>
ISDN (Integrated Services Digital Network).................................................................7
IT security..................................................................................................................17-20, 22
LAN (Local Area Network)...........................................................................................6, 7, 9, 12, 15, 23
MAC (Media Access Control)........................................................................................10
MacOS (Macintosh Operating System)...........................................................................20
NAT (Network address Translation)..............................................................................14, 20
network access layer......................................................................................................6, 15, 21
network layer..................................................................................................................8, 20
NTP (Network Time Protocol).........................................................................................9, 15
operating system............................................................................................................12, 15, 17, 20
OS (Operating System)..................................................................................................20
packet filter....................................................................................................................6, 7, 13, 14, 21, 22
PAP (Paketfilter – Application-Level Gateway – Paketfilter)........................................13, 14
patch..............................................................................................................................21
protection requirement.................................................................................................6, 7, 13-15, 21
protocol..........................................................................................................................8-11, 15, 19-21, 23
proxy..............................................................................................................................21
redundancy......................................................................................................................14
residual risk......................................................................................................................15
risk...................................................................................................................................15
router............................................................................................................................6, 9, 14, 21
routing.............................................................................................................................9
security concept............................................................................................................14, 16, 21, 22
security gateway...........................................................................................................6, 11-14, 22
security policy................................................................................................................22
security safeguards.........................................................................................................14, 22
security zone...................................................................................................................14
segmentation..................................................................................................................9, 11, 13
server..............................................................................................................................22
service provider.............................................................................................................22
SFTP (SSH File Transfer Protocol) ................................................................................9
SMTP (Simple Mail Transfer Protocol).........................................................................8, 17, 22
sniffing...........................................................................................................................6, 10, 11, 22
SNMP (Simple Network Management Protocol).........................................................9, 14
SNMPv3 (Simple Network Management Protocol Version 3).....................................9, 10
spoofing..........................................................................................................................6, 10, 11, 22
SSH (Secure Shell).......................................................................................................6, 10, 14
switch............................................................................................................................10, 22
TAN..................................................................................................................................10
TCP (Transmission Control Protocol)............................................................................6, 8-10, 15, 17, 19-21, 23
telnet (Teletype Network)............................................................................................9, 10
threat..............................................................................................................................7, 8, 10, 17, 23, 24
transport layer................................................................................................................20, 23
TTL (Time to live)..........................................................................................................8
TV (Television)...............................................................................................................8
UDP (User Datagram Protocol)......................................................................................8, 10, 19, 23
URL (Uniform Recource Locator)...............................................................................19
URL (Uniform Resource Locator)................................................................................19
VLAN (Virtual Local Area Network)............................................................................13, 23
VPN (Virtual Private Network)....................................................................................7, 23

Federal Office for Information Security
vulnerability..............................................................................................................................9, 17, 24
web (WWW (World Wide Web))...........................................................................................6, 7, 14, 19, 22
Whitelist.............................................................................................................................................12
World Wide Web......................................................................................................................................7
WWW (World Wide Web).......................................................................................................................7, 14