

**RECOMMENDATION ON THE
APPLICATION OF REGULATION FICORA
13 A/2008 M**

**ON INFORMATION SECURITY AND
FUNCTIONALITY OF INTERNET ACCESS
SERVICES**

CONTENTS

- 1. SCOPE OF APPLICATION 2**
- 2. DEFINITIONS..... 2**
- 3. INFORMATION SECURITY IN CUSTOMER SUBSCRIPTIONS 3**
 - 3.1. INFORMATION TO CUSTOMERS..... 4
 - 3.2. INFORMATION TO CUSTOMERS REGARDING TECHNICAL RESTRICTIONS OF THE SUBSCRIPTION 5
- 4. DIRECTING AND ROUTING OF E-MAIL TRAFFIC TO A CONSUMER SUBSCRIPTION 5**
- 5. DIRECTING AND ROUTING OF OUTGOING E-MAIL TRAFFIC FROM A CONSUMER SUBSCRIPTION 6**
- 6. ADDRESS-BASED FILTERING IN CUSTOMER SUBSCRIPTIONS 7**
- 7. DETECTION AND FILTERING OF MALICIOUS TRAFFIC IN CUSTOMER SUBSCRIPTIONS 7**
 - 7.1. DETECTION OF MALICIOUS TRAFFIC 7
 - 7.2. PROCESSES AND OPERATIONS MODELS FOR TEMPORARY TRAFFIC FILTERING 8
 - 7.3. DISCONNECTION OF CUSTOMER SUBSCRIPTIONS..... 8
- 8. INFORMATION SECURITY OF A BACKBONE NETWORK..... 10**
- 9. ADDRESS AND ROUTE FILTERING IN A BACKBONE NETWORK 11**
 - 9.1. VERIFYING ROUTE ADVERTISING..... 11
 - 9.2. FILTERING OF TRAFFIC WITH INCORRECT SOURCE ADDRESSES 11
 - 9.3. FILTERING OF DIRECTED BROADCAST TRAFFIC 11
 - 9.4. DOCUMENTATION OF ADVERTISED NETWORKS 11
 - 9.5. FILTERING OF UNUSED ADDRESS SPACES 12
- 10. DETECTION AND FILTERING OF MALICIOUS TRAFFIC IN A BACKBONE NETWORK..... 12**
- 11. MONITORING OF FUNCTIONALITY AND QUALITY OF INTERNET ACCESS SERVICES 13**
 - 11.1. SIGNIFICANT EXCEPTIONAL EVENTS THAT AFFECT THE AVAILABILITY OF THE COMMUNICATIONS NETWORK OR COMMUNICATIONS SERVICE 13
 - 11.2. NETWORK LOAD 13
 - 11.3. INTERRUPTIONS IN THE INTERNET ACCESS SERVICE SORTED PER TYPE..... 13
 - 11.4. DETECTED FAULTS IN INDIVIDUAL CUSTOMER SUBSCRIPTIONS SORTED PER TYPE..... 13
 - 11.5. NUMBER OF SUBSCRIPTIONS DISCONNECTED ON THE BASIS OF THIS REGULATION 13
- 12. OPERATOR'S CONTACT INFORMATION IN PUBLIC IP ADDRESS REGISTERS 14**

1. SCOPE OF APPLICATION

The Regulation applies to the production of Internet access services provided in public communications networks and to related systems, communications networks and communications services used by telecommunications operators to provide these services. In this regulation, Internet access service means transmission of Internet traffic.

The regulation applies, as applicable, to the production of Internet access services both for network operators and for service operators.

The information security measures provided in the regulation must, according to section 19 of the Act on the Protection of Privacy in Electronic Communications, be commensurate with the seriousness of threats, level of technical development and costs.

2. DEFINITIONS

In this Regulation, "customer subscription" means the logical interface between a customer network and the Internet, intended to be used both by consumers and by companies. The subscriber of the customer subscription is connected to the public communications network and its services via the customer subscription.

In this regulation, "interface between the customer subscription and the Internet" means the logical interface separating two different networks or an individual user and the network. Technically, the interface is located between the customer network and the network operator's network, and between the network operator's network and the service operator's network. The logical interface may also be located between the customer's virtual network and the public Internet.

A customer subscription may be implemented using several alternative technologies, such as analogue dial-up modem, radio network, wireless local area network, cable data network or DSL.

The interfaces involved in the implementation of a subscriber connection are illustrated in the following figure.

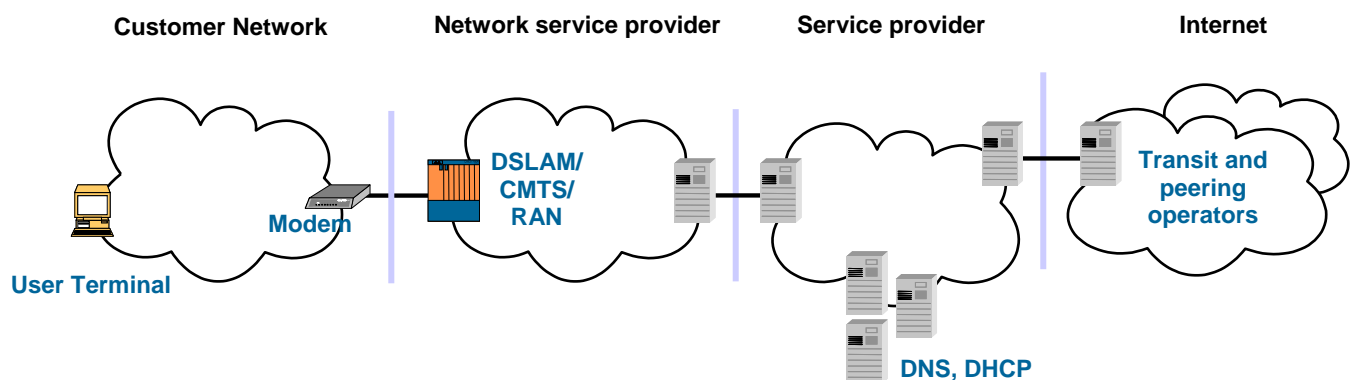


Figure 1: Example of network interfaces

In this regulation, "customer subscription services" mean services that a telecommunications operator provides to its customers via the customer subscription for delivering Internet traffic.

Services provided through the customer subscription to deliver Internet traffic are, for example, domain name service (DNS), Dynamic Host Configuration Protocol (DHCP) for assigning Internet addresses, Simple Mail Transfer Protocol (SMTP) and proxy. The services may either be supplementary services to the subscription or necessary for the use of the subscription, such as the name service.

In this regulation, "transit traffic or transit service" means service that a telecommunications operator provides to its customers or another operator to exchange or deliver Internet traffic.

On the Internet, several operators have an autonomous system (AS) and are connected to many other similar networks through various public or private exchange or transmission agreements. The networks communicate with each other by using the Border Gateway Protocol (BGP).

Networks of equal size can normally exchange traffic with each other without compensation through peering. Part of the exchange is carried out as chargeable transit traffic, especially when all Internet routes are advertised to another operator.

Interconnection of traffic is typically carried out through multiple interconnection points to ensure communication.

In this regulation, "filtering" means prevention or restriction of Internet traffic in accordance with predefined rules.

Filtering can, for example, mean rejection of outgoing Internet traffic from a customer subscription that has forged source addresses. It is possible to detect forged addresses by comparing the source addresses with the address spaces granted to the customer.

Filtering can also mean restriction of the capacity of certain Internet traffic based on subscription type or application protocol used.

It is possible to filter traffic without the consent of the service user if the measures are necessary to maintain information security or to prevent a threat against the availability or information security of the communications network or service. When an operator implements the filtering measures, it must not only take into account Chapter 5 of the Act on the Protection of Privacy in Electronic Communications but also the requirements imposed in the Consumer Protection Act (38/1978) and Communications Market Act (393/2003).

3. INFORMATION SECURITY IN CUSTOMER SUBSCRIPTIONS

A telecommunications operator must perform the implementation and maintenance of customer subscriptions in such a manner that information security aspects are taken into consideration.

When a telecommunications operator provides a customer subscription with shared capacity with other subscribers, it must separate the subscribers' traffic in such a way that the subscribers cannot unlawfully monitor each others' traffic. An operator must ensure that unauthorized redirection of another subscriber's traffic between the subscriptions is not possible.

Shared Internet capacity among subscribers is typical in the implementation of housing companies' networks. In these solutions, the Internet connection brought into the housing company is shared among the users within this housing company either by using the housing company's network equipment or the operator's network equipment. Corresponding network implementations with shared capacity are typical, for example, in metropolitan area networks (MAN), where the service is open to all users within the network coverage area.

Traffic restrictions are simpler to arrange in community networks than in corporate networks, because community network users do not often need to communicate directly with each other but the traffic is usually outbound-directed.

The subscribers' traffic can be separated from each other e.g. by defining apartment-specific ports of the housing company's Ethernet or HomePNA switches to separate Virtual LANs (VLANs). Alternatively, traffic between apartment-specific ports can be blocked in switches.

Operators should inform the customers about information security risks related to shared capacity when the operator itself does not implement this kind of access, where the capacity is shared between the users. Information liability may, for example, refer to situations where the operator only implements the Internet connection to the housing company and the housing company, as a corporate or association subscriber, is responsible for the capacity sharing.

When an operator implements the Internet access using technology that by default does not support separation of subscribers' traffic from each other (e.g. hotspot-like unencrypted WLAN (Wireless Local Area Network) solutions), information security must be maintained in other ways, for example by informing the users of risks related to unencrypted communication.

As stated above, for example for WLAN, it is not always possible to eliminate all information security threats to the service. Also in these situations, the operator is liable to inform the customer about the threat. According to section 19 of the Act on the Protection of Privacy in Electronic Communications, the measures intended to maintain information security of the operator's communications and network service must be commensurate with the seriousness of threats, level of technical development and costs.

3.1. Information to customers

Prior to connecting the customer subscription, a telecommunications operator must inform the customer about the general information security risks and risks related to the specific subscription type, and about the available methods to ensure information security.

The information has to focus on the measures available to the customer or user of the subscription to maintain information security. Such measures are, for example, the use of a personal firewall prior to connecting the computer to the network, antivirus software and updates of the operating system and other software/network services. An operator may have included these solutions in an information security service package including a personal firewall and antivirus software provided to customers.

Customers must also be informed of relevant information security threats affecting the user and where it is possible to get further information about security issues related to the use of the subscription. The customer must be informed of the operator's contact information for problem situations, for example for cases where the subscription is disconnected from the public communications network or where there are other information security issues related to the use of the subscription.

Customers can be informed in several ways. For example, in service descriptions of subscription types, or when the subscription is being ordered, the subscription type is being changed, the order is being acknowledged or the subscription is being delivered. The most important thing in informing the customer is that the customer has relevant information, preferably in written form, before the subscription is connected to the communications network, and no later than when the subscription is delivered. General information of information security on the operator's website does not fulfil these requirements, as the customer's system is likely to be infected with malware before he or she is even able to access the instructions.

If an operator provides customer subscriptions with no traffic restrictions, the customer must be informed of the specific risks related to the use of the subscription. These risks mean here, for example, information security risks related to server maintenance.

Specific information security risks for unrestricted incoming traffic are often related to hardware and software security issues in server maintenance, such as software updates, restriction of access rights, and the server maintenance itself. For unrestricted outgoing traffic, information security risks often relate to spam traffic caused by malware infected workstations.

3.2. Information to customers regarding technical restrictions of the subscription

A telecommunications operator must define a clear policy of use for customer subscriptions and describe it to the customer. The description must contain the essential technical restrictions affecting the use of the customer subscription, for example, permanent restrictions related to communication ports, protocols and traffic volume, and traffic restrictions for the specific subscription type. The description must also include the actions to be taken in case the subscription or services are used in an exceptional manner.

Protocol-specific traffic restrictions can mean, for example, that traffic volume of certain application protocols is limited to a certain amount of subscription capacity.

These characteristics are part of the basic qualities of the specific subscription type. In addition to the basic characteristics of the subscription, it is also possible to maintain customer subscription's information security by means of temporary measures, which will be referred to below.

Customer subscriptions to consumers can be divided as follows:

- - protected subscription where all incoming connections and certain ports of outgoing traffic are blocked
- - power user subscription where certain ports of the incoming traffic are blocked and outgoing traffic is mainly allowed
- - unprotected subscription where unrestricted traffic is mainly allowed.

A description of the basic characteristics of a subscription must be given to the customer, for example, in the product description so that the customer can choose the most suitable subscription. The basic description can include information about blocked network ports and prioritization of certain application protocols in the specific subscription type. If application protocols are prioritized, the customer must, at a general level, be informed of the principles of traffic prioritization and of the capacity which is available for different applications.

The description can be made, for example, by issuing an acceptable use policy and limitations for allowed network usage in the subscription agreement and by describing the changing use restrictions on a separate information page on the operator's website.

For setting or changing usage limitations during the validity of the subscription agreement, an operator must take into account the contents of the agreement and follow the procedures given in the legislation, if the limitation comes as a unilateral change to the agreement.

The use policy must, in addition to traffic restrictions, include the actions to be taken in case exceptional communication is detected. When the operator uses an automatic system for traffic management, for example by putting customer subscriptions in quarantine when they communicate in an exceptional manner, operators must give a general explanation to the customer of what the limitations are when a user is put in quarantine, how long the subscription is isolated, and what the requirements are to allow return to normal communication. The definition of traffic limitations must not endanger information security of the communication service, that is, the description must not be unnecessary detailed giving exact grounds when certain type of traffic is regarded to be malicious.

4. DIRECTING AND ROUTING OF E-MAIL TRAFFIC TO A CONSUMER SUBSCRIPTION

A telecommunications operator providing Internet connections must prevent incoming SMTP (Simple Mail Transfer Protocol) traffic to a consumer subscription from elsewhere than through agreed servers intended for SMTP traffic. Prevention of SMTP traffic means, for example, denying traffic from outside the operator's network to the data communications port reserved for SMTP traffic or directing it to servers intended for incoming SMTP traffic. The traffic can also be restricted

in the telecommunications operator's network, i.e. between different subscription types, for example between corporate and consumer subscriptions.

The purpose of the prevention measures is to prevent the use of open relays that can be installed automatically by possible malware in consumer subscriptions from outside the telecommunications operator's network. Furthermore, preventive measures are necessary for the prevention of break-in to vulnerable e-mail servers possibly incorporated in consumer subscriptions from outside the telecommunications operator's network by exploiting the vulnerability of e-mail applications or servers.

Some consumer subscribers may, however, have needs for direct SMTP traffic to a consumer subscription. A telecommunications operator may allow incoming SMTP traffic to the subscriber connection from elsewhere than through the agreed servers intended for SMTP traffic. In this case, a telecommunications operator must inform the subscriber of the risks related to open communications and the measures the user may take to have control of the risks.

Direct SMTP traffic to a consumer subscription may be needed for e.g. in cases where a consumer subscription has an e-mail server approved by a telecommunications operator and e-mail cannot be routed to the server concerned through the operator's own e-mail system. Since it is a server system receiving e-mail traffic from an unrestricted network space, it is utterly important to see to the information security of the service. This means that the system set-up is correct and software upgrades are done.

5. DIRECTING AND ROUTING OF OUTGOING E-MAIL TRAFFIC FROM A CONSUMER SUBSCRIPTION

A telecommunications operator providing Internet connections must prevent unrestricted outgoing SMTP traffic from consumer subscriptions otherwise than through agreed servers intended for outgoing SMTP traffic. The prevention of unrestricted SMTP traffic means e.g. that traffic directed to the communications port reserved for SMTP traffic outside the operator's network originating from the network space a telecommunications operator has meant for consumer subscriptions is blocked or directed to servers meant for outgoing SMTP traffic. The traffic can also be restricted in the telecommunications operator's network, i.e. between different subscription types, for example between corporate and consumer subscriptions.

Outgoing SMTP restriction can be implemented e.g. by software which is used to automatically manage outgoing SMTP traffic by the telecommunications operator e.g. by delaying traffic or denying traffic partly or totally from subscriptions sending uncontrolled SMTP traffic. This means, for example, that the volume of traffic sent from a consumer subscription is exceptionally large or the number of recipients is very high.

When unrestricted outgoing SMTP traffic is routed to external networks through servers intended for outgoing SMTP, these systems allow efficient control of traffic volumes.

The e-mail system of a telecommunications operator must not prevent the use of other domain names than those administered by it as a part of the sender's domain name in outgoing e-mail messages addresses. The customers must be allowed to freely use domain names of third parties in their communications.

Restriction of SMTP traffic accomplished in compliance with the regulation must not affect e-mail communications using other data communications ports, such as e-mail protocols using a user authentication or encryption. Thus, the customers of a telecommunications operator providing Internet connections may safely communicate with an e-mail system under another service provider's administration.

Some consumer subscribers may have justified needs for direct SMTP traffic from the consumer subscription to any external network. A telecommunications operator may allow unrestricted

outgoing SMTP traffic even otherwise than through the agreed servers intended for outgoing SMTP traffic. In this case, an operator must inform the subscriber of the risks related to open communications and particularly monitor the volume of outgoing SMTP traffic from the subscriber connection in its communications network. Then, an operator must also be prepared to react rapidly to disruptions.

Primarily, outgoing SMTP traffic from e-mail servers in consumer subscriptions can also be routed through servers intended for outgoing SMTP traffic, but in certain cases direct communication may be needed. In this regulation, monitoring of outgoing SMTP traffic from consumer subscriptions means automatic control of traffic volumes and methods, and interference in the communication on the basis of the monitoring.

6. ADDRESS-BASED FILTERING IN CUSTOMER SUBSCRIPTIONS

In distributed denial-of-service attacks, the attackers often try to make finding the source of the attack difficult by using random source addresses in the attack traffic. It is possible to make an external network or randomly chosen address in the target network look like the source of the attack by spoofing the source addresses. The spoofed source addresses may also be randomly selected from address spaces reserved for private use or for special purposes.

In order to block traffic that uses forged source addresses, the operator providing customer subscriptions must filter outgoing traffic from a customer subscription to the communications network in cases where the source address has not been assigned to this particular customer subscription. An operator must, if necessary, be able to find out the customer subscription sending forged traffic.

Filtering can be implemented by comparing the source address of each packet received at the interface with the list of acceptable address spaces and by rejecting each packet whose source address does not belong to the address spaces in the list.

An operator providing customer subscriptions should also filter traffic from the external communications network to the customer subscription when the source address of the traffic is from the address space of the specific subscription (RFC 3013, items 4.3 and 4.4, and RFC 3704 for multihoming networks).

The operator must perform the filtering in the network element which is closest to the customer interface and where it is technically most feasible. The filtering must, where possible, also be performed between the operator's customers.

For ADSL connections, filtering can take place in the DSLAM network element of the concentrator, in the network equipment terminating DSL network connections, or in the router of the backbone network. The feasibility of filtering depends on the technical filtering capacity of the network equipment, or the operator's filtering practices.

7. DETECTION AND FILTERING OF MALICIOUS TRAFFIC IN CUSTOMER SUBSCRIPTIONS

7.1. Detection of malicious traffic

A telecommunications operator must monitor and, when necessary, resolve the events in its own communications network in order to detect traffic that endangers the information security or availability of the communications network or communications service.

An operator must define a group responsible for the information security of the communications network and/or services and to whom contacts regarding customer subscriptions from customers and external instances can be directed regarding incidents that may endanger information

security, and who also monitors communications network incidents and is responsible of incident resolution.

An operator may be informed of a customer subscription sending traffic that endangers the information security or availability of a communications service in several ways, for example, through the automatic system controlling traffic volumes and deviations from normal volume; through a disturbance situation in a communications service; through a notification from an external instance; or through a complaint from a customer. An operator must verify the validity of the notifications in an appropriate manner.

An operator must specify the procedures and ways of contact, according to which the group responsible for the information security of the communications network cooperates and, where necessary, exchanges information with other Internet service providers, customers and authorities about incidents that may endanger information security of the communications service. An operator must agree on the methods for secure information sharing in advance with the most important cooperation partners.

7.2. Processes and operations models for temporary traffic filtering

An operator may be informed of a situation which threatens information security or availability of a communications network or communications service in above mentioned ways. An example of such a situation is when fast-spreading malware causes traffic directed to a specific communication port.

In this situation, an operator may have to adopt temporary measures in order to block traffic to and from customer subscriptions directed to the specific communication port or to restrict traffic from customer subscriptions to certain destination addresses. A telecommunications operator must have processes and operations models for temporary filtering of customer subscriptions traffic in situations which endanger the information security or availability of the communications network or communications service.

An operator must inform users about the actions on the Internet service provider's website. Filtering actions must be interrupted as soon as the severe threat that endangered information security or availability of the communications network or communications service has ended.

7.3. Disconnection of customer subscriptions

A telecommunications operator must disconnect a customer subscription or its service from the public communications network, if the subscription essentially endangers information security or availability of the communications service. Disconnection and reconnection of the subscription must be carried out in accordance with the predefined processes and guidelines. Special circumstances due to the subscription type may be taken into consideration when the measures are implemented.

In this regulation, disconnection of a service from the public communications network means that certain communication ports of a customer subscription are temporarily closed when traffic directed to these ports endangers information security or availability of the communications service. An operator may also have to restrict traffic of certain application protocols from a customer subscription if traffic endangers information security or availability of the communications service.

The activities of a customer subscription may essentially endanger information security or the availability of the communications service, for example, in situations where a malware-infected system attached to the customer subscription sends large volumes of spam or malware. The infected system may also endanger information security or availability of the communications service, if it is used for a denial-of-service attack where the system sends traffic that endangers the communication service's information security or traffic that is used to prevent communication for a certain party.

An open mail relay maintained in the Internet subscription can also be regarded to endanger the information security or usability of a communications service. A telecommunications operator is obliged to disconnect from the public communications network an information system acting as an open mail relay it has detected or been informed of, when this is necessary with regard to the information security or availability of the service.

A telecommunications operator may be informed of an open mail relay in its network e.g. through the monitoring of its own e-mail system or communications network, by an external party's announcement or through a customer. An operator must appropriately verify the reliability of the information before disconnecting the system from the public communications network.

A customer subscription does not typically endanger the information security or availability of the communications service when the customer subscription or a www service connected to the network through the customer subscription is a target for a denial-of-service attack and therefore receives exceptionally large volumes of traffic in a certain situation. Such situations are handled according to procedures described below.

When maintaining information security and disconnecting customer subscriptions, it should be noted that right to process identification data in communications only applies in situations that threaten or violate the information security of communications networks and services. The operator does not have a general right to monitor the contents of customers' traffic or identification data in any other cases.

If an operator by other means than through processing of identification data in confidential communication finds out that the customer's communication endangers other persons' rights in a criminal manner, the conditions of the subscription agreement and legislation applicable to the contractual relation must be followed.

Actions related to disconnection have to be done according to the operator's predefined processes. The actions taken and especially the reason for disconnection must be registered in case the situation needs further clarification afterwards. Where possible, the operator must contact the customer by phone or e-mail before the subscription is disconnected from the public communications network. However, is not always possible to contact the customer, for example, in situations that demand fast response when the service's information security or availability is severely threatened. In these situations, contacting the customer must not unnecessarily endanger the information security or availability of the service.

Disconnection and reconnection of the subscription must be carried out in accordance with the predefined processes and guidelines. Special circumstances due to the subscription type may be taken into consideration when the measures are implemented. For example, when the subscription type is intended for service providers, it may be best for the parties to agree on the operations models for fault situations in such a manner that the damages to the provision of the services are as slight as possible.

The disconnection guidelines should include all the necessary procedures to reconnect the customer subscription to the communications network, when an operator has decided that the threat to the communications service has ended. For example, when malware causes malicious traffic, the subscription can be reconnected to the communications network after the customer has contacted the operator and informed that the system has been cleaned.

The service and network operator should agree on the principles related to the implementation of the disconnection process. Both parties should be able to take all necessary actions to maintain the information security of a service or network. The other party must be informed of disconnection and reconnection without delay.

When the customer subscriptions are monitored automatically, the subscriptions or certain services related to a subscription are usually disconnected when necessary from the public communications

network automatically without operator's actions for example for 30 minutes when limits set to malicious traffic are exceeded. After the customer's subscription is disconnected, traffic may be routed to a restricted area where the customer is informed of the reason for disconnection and possible measures that the customer may have to take in order to fix his or her equipment. The customer may also be able to go to certain websites to install an anti-virus program and to update the operating system. This operation model reduces the necessity for a more permanent disconnection of customer subscriptions.

When automatic systems are used to close and open customer connections to maintain information security and availability of the service, the customer must be informed of the principles related to the temporary closing and opening as described in chapter 3.

8. INFORMATION SECURITY OF A BACKBONE NETWORK

A telecommunications operator must have instructions and operation models for denial-of-service attacks and other events that may endanger the information security or availability of the communications network or communications service.

The operator's guidelines and other procedures for denial-of-service attacks and other events that may endanger the information security or availability of the communications network or service must be so precise that the operator's personnel can react to the most typical exceptional events and act according to the given procedures and guidelines.

A telecommunications operator must be prepared to take action in order to restrict traffic related to denial-of-service attacks and to trace traffic with incorrect source addresses.

An operator's network must support traffic volume restrictions so that information security and availability of the service can be maintained.

Traffic restriction measures mean, for example, that Internet service provider's network elements support the restriction of traffic volume based on a specific protocol, address, port and network. These measures can prevent denial-of-service attacks and restrict the damages caused by certain network attack methods.

Traffic restriction measures may, for example, restrict the effects of such denial-of-service attacks where certain kind of malicious traffic is used to load the network systems. The measures may also be used to restrict malware traffic directed to a certain port.

To be prepared to trace traffic means, for example, that an operator creates such operations models and practices that enable the discovery of the origin of traffic that uses incorrect source addresses. The measures may include instructions and necessary modifications to the settings of the backbone network equipment.

The purpose of tracing the origin of traffic that uses incorrect source addresses is to recognise the device sending traffic to prevent the disturbances caused to information security of the service because of malicious traffic related to the denial-of-service attack.

Network elements that restrict traffic volume must support the restriction both for traffic towards the network element itself and traffic going through the network element. Traffic volume restrictions must be implemented without unnecessary endangering of the network availability. Network element that restricts traffic must be able to perform the measures, such as IP traffic filtering, without creating unreasonable load to the network element.

Network elements that restrict traffic volume must, where necessary, be able to register the relevant event log data about filtering, such as the source and target address, source and target port, and how the packet was handled. In assessing relevance, attention must be paid to adequate sampling accuracy. In some cases, it may be sufficient to record every tenth packet out of the

filtered traffic. Logging is necessary for problem resolution, network attack investigation and identification. The network element must support logging to a centralised log server. The event log data must be time stamped and a centralised time source must be used for timing.

9. ADDRESS AND ROUTE FILTERING IN A BACKBONE NETWORK

The telecommunications operators who exchange traffic must prevent the transmission of such traffic where the source address is not in the route advertising of the submitting operator.

The main responsibility for blocking the transmission of traffic that uses incorrect source addresses rests with the submitting operator.

9.1. Verifying route advertising

Routes which belong to the telecommunications operator's own networks must be filtered from received route advertising, unless otherwise agreed for a specific network.

No other operator should advertise the operator's own or more specific routes without a special agreement; for example, certain temporary multihoming solutions may require such advertising. Unlawful advertising may be intentional to route traffic to the attacker's system, or it may also be unintentional. In order to protect itself against the threat caused by unjustifiable advertising, an operator receiving route advertisements must filter the incorrect advertisements.

9.2. Filtering of traffic with incorrect source addresses

A telecommunications operator must filter such incoming traffic to its own communications network where the source address has been assigned to this particular operator, unless otherwise agreed for transmission of such traffic. Filtering must be performed with a technically feasible accuracy.

Packets which have incorrect source addresses have either been sent as a consequence of incorrect address definition or deliberate source address spoofing.

In some exceptional cases, an operator may agree with another operator upon that a part of the operator's address space is temporarily routed as coming from the other operator's network.

9.3. Filtering of directed broadcast traffic

A telecommunications operator must prevent, at network interfaces, the distribution of broadcast messages intended for network elements connected to the public Internet. Ethernet is an example of a network where directed broadcast messages are typically used.

9.4. Documentation of advertised networks

A telecommunications operator must carefully document the use of all advertised addresses assigned to it by registering the networks with a public Internet Routing Registry (IRR).

It is important to register advertised address spaces because operators use this information to create automatic prefix lists for route filtering. The prefix lists ensure that an operator advertising routes only advertises those address spaces that it manages. Carefully-entered address information also contains the contact person responsible, for example, for abuse contacts.

Public documentation must be carried out at least with the accuracy of the advertised routes. The registration is entered in the RIPE database by means of valid methods. Undocumented address spaces must not be advertised to other operators.

A telecommunications operator providing transit service must see to that the customer networks it advertises are registered with the public Internet Routing Registry (IRR) in accordance with principles stated in the previous item of this Recommendation.

Although the customer organisations might manage the address spaces or routing themselves, they would not necessarily be aware of this regulation and recommendation and of the methods, according to which the use of address spaces must be registered with the Internet Routing Registry. An operator providing transit service is also responsible for giving advice to the customers where needed so that registration of customer networks is also performed correctly.

9.5. Filtering of unused address spaces

When a telecommunications operator uses filtering rules based on unused address spaces or those reserved for special purposes to filter traffic or routes, it must ensure that the filtering rules are up-to-date.

Route advertising can be filtered to prevent unused address spaces from being hijacked. Also, traffic can be filtered on the basis of source addresses for the purpose of filtering traffic with regard to denial-of-service attacks. As denial-of-service attacks regularly use spoofed but routable source addresses, the need for address filtering and update mechanisms should be carefully considered.

Examples of address spaces to be filtered can be the so-called bogon prefixes which mean address spaces meant for private use (RFC 1918) or for special purposes. Filterable address spaces may also be networks, which the Internet Assigned Numbers Authority (IANA) or the local Internet address registries have not yet allocated.

When route information or traffic is filtered, an operator must see to that the filtering ruleset is up-to-date in order to prevent recently allocated address spaces from being filtered. For Bogon filtering it is possible to use Border Gateway Protocol (BGP) feed provided by reliable parties where changes to address spaces are made to the ruleset in a concentrated manner.

Default bogon lists provided by some routers must not be used because they are out-of-date.

10. DETECTION AND FILTERING OF MALICIOUS TRAFFIC IN A BACKBONE NETWORK

A telecommunications operator must monitor and, where necessary, resolve the events in its own backbone network in order to detect traffic that may endanger the information security or availability of the communications network or communications service.

An operator must define a group responsible for the information security of the communications network and/or services and to whom monitoring and response of incidents that may endanger information security in the backbone network can be directed. An operator may be informed of events that endanger the information security of a communications service, such as denial-of-service attacks done through the backbone network or malware that causes an exceptional volume of traffic, through own monitoring or through a notification from an external party.

An operator may use an automatic control system that monitors backbone traffic volume or exceptional events in its event monitoring. In addition, intrusion detection and intrusion prevention systems may be used to manage security incidents.

An operator must define the methods according to which the group responsible for backbone network security cooperates and exchanges information about incidents endangering the information security of a communications service with corresponding groups of other Internet service providers, with authorities, other information security players, such as CERT groups, and parties responsible for information security of customer subscriptions. An operator must establish

secure information exchange methods with the most important cooperation partners in order that problem situations can be solved quickly.

11. MONITORING OF FUNCTIONALITY AND QUALITY OF INTERNET ACCESS SERVICES

A telecommunications operator must continuously monitor the quality and reliability of the Internet access services it provides. Monitoring of the availability and quality of services supports the management and development processes of the services, and the availability of services. The monitoring function can also be used to indicate how the agreed service quality is fulfilled.

11.1. Significant exceptional events that affect the availability of the communications network or communications service

Monitoring of significant exceptional events means that those events which have caused significant deviations in the network or service availability or information security are reported and that statistics are compiled on them. Such events may be errors in the network backbone equipment or significant deviations in service quality caused by massive denial-of-service attacks.

11.2. Network load

Measuring the network load means that the status of the telecommunication network is monitored so as to define and report the load. Monitoring of the network status means, for example, that the capacity of the backbone network or the load of a specific subscription is monitored. It may also mean that total traffic volumes of individual ADSL subscriber connections are monitored so as to ensure sufficient capacity.

11.3. Interruptions in the Internet access service sorted per type

Monitoring and sorting of interruptions in the Internet access service mean that both unplanned and planned exceptional interruptions are registered in accordance with predefined procedures.

Interruptions can be sorted as follows:

- - Hardware faults
- - Software errors
- - Configuration errors
- - Faults caused by load
- - Faults and interruptions caused by denial-of-service attacks

11.4. Detected faults in individual customer subscriptions sorted per type

Faults detected by an operator in an individual customer subscription can be sorted by type in the same way as in the whole Internet access service. Individual customer subscription may be a single subscriber-specific ADSL or cable modem subscription.

Faults can be sorted as follows:

- - Hardware faults
- - Software errors
- - Configuration errors
- - Cable faults

11.5. Number of subscriptions disconnected on the basis of this Regulation

Monitoring of the number of subscriptions disconnected on the basis of this Regulation means examination and statistics compilation of the disconnected customer subscriptions or other customer connections. Correspondingly, it is possible to monitor the number and restriction mechanisms of those customer subscriptions which are targets for the automatic traffic control

system because as these subscriptions have sent traffic which may endanger information security of the service.

When an operator monitors these subscriptions and the various actions it can measure the state of the network with regard to information security, it can compile statistics on the relevant values for the reports and it can also intervene in the deviations, where necessary. The monitoring of disconnected subscriptions must be related to the processes of disconnection defined by the operator. The reason for disconnection or restriction must be taken into consideration in the monitoring, time for disconnection, person who performed the disconnection, measures that have been taken, contacting the customer, and time for reconnection.

12. OPERATOR'S CONTACT INFORMATION IN PUBLIC IP ADDRESS REGISTERS

A telecommunications operator must see to that the WHOIS database of the Regional Internet Registry (RIR), who assigned the IP address block, contains relevant contact information regarding address spaces allocated to the operator or operator's customers, abuse information included.

A telecommunications operator must see to that the contacts made on the basis of the abuse information with parties responsible for the management of address spaces in the possession of the operator or operator's customers are registered and that the contacts are regularly monitored.

As contact information in the Regional Internet Registry are public, large volumes of spam and other irrelevant communication is sent especially to the abuse e-mail addresses. Therefore, the messaging should be handled with an automatic tool, which filters irrelevant messages and registers and acknowledges other contacts. This will simplify the resolution process and make it more effective.