Security requirements for suppliers of infrastructure equipment and service platforms

Fédération française des télécommunications

29 May 2018

Purpose of the document

This document describes the security requirements operators that are members of the FFT must demand from their suppliers of infrastructure equipment and service platforms, and their service providers.

This document applies to all the assets of every telecommunications operator. It includes requirements for the products and the services provided during their integration, operation and maintenance.

The security requirements described in this document are drawn from the document referenced, including those related to the administration workstation for technical systems, an area that requires special attention from suppliers.

These requirements form a common base. Each operator may customise the base and add its own requirements depending on its architecture and SOC services.

Furthermore, for a critical information system, it is necessary to make sure that the supplier - or their service provider - as subcontractors of the operator, comply with all the applicable rules in the reference document.

Reference

This document is based on the Order of 28 November 2016, setting the security rules and the method for declaring critical information systems and security incidents concerning the sub-sector of critically important 'Electronic Communications and Internet' activities, for the application of Articles R. 1332-41-1, R. 1332-41-2 and R. 1332-41-10 of the French Defence Code, published in the Official Gazette n° 0282 on 04/12/2016.

Governance requirements

Mapping

The operator may ask the supplier to provide information required to compile the mapping of the asset, such as, for example, the plans for the internal flows of the asset, the mapping of the applications implemented on the asset, the list of physical components comprising the asset, etc.

Suppliers should note that the mapping information for the assets consists of confidential documents possibly containing information that may not be divulged under the terms of Article 226-13 of the French Criminal Code.

It is incumbent upon the supplier to achieve compliance to protect the confidential mapping data on the technical system deployed by the operator for example if the asset is a component of a critical information system as per the meaning of Article R1332-41-2 of the French Defence Code.

If the data are classified or subject to marking, then the supplier must have adequate means of storage for example the supplier may refer to Inter-ministerial Instruction (IGI) 1300 for the management requirements for data classified "Confidential Defence" (CD) - and follow the instructions for marking the document (e.g. "Special France").

Maintenance of the asset in secure conditions

Logging

Security events regarding user authentication, management of accounts and access rights, access to resources, modifications to the security rules for the asset, and the functioning of the asset, are saved in a log management system for a period of at least 6 months.

To do so, the operator connects the asset to a log management system external to the asset itself. The asset must thus implement mechanisms like SFTP or syslog making it possible to send the security events to the operator's logging system.

The operator also expects the supplier to document the security events of the asset to make them exploitable by a Security Information and Event Management (SIEM) system. The logs corresponding to serious events such as the detection of an intrusion into the asset must be detailed. The time-stamp system for the events must be controlled by a time source external to the asset, using the Network Time Protocol (NTP), for example. Should the events need to be stored locally on the asset, the supplier shall document and justify any exceptions to the retention period.

Managing vulnerabilities

The operator asks the supplier to write down in a procedure the conditions needed to maintain the level of security of the asset resources depending on changes to the vulnerabilities and threats. In particular, the supplier must describe the installation policy for any new version, the corrective security measures for a resource and the verifications to be carried out prior to installation.

The supplier undertakes to implement a process to:

- identify the vulnerabilities linked to the Operating System (Windows, Linux) and the applications - on the technical systems comprising the asset, for example by monitoring alerts from different CERTs and publishers;
- analyse the criticality of the vulnerability and determine the priority for the application of a patch;
- warn the operator immediately and via a dedicated channel (encrypted message or CERT, for example);
- propose a bypass plan followed by a definitive patch within the time-frame specified in the maintenance contract depending on the criticality of the anomaly, as agreed between the operator and the supplier.

Managing security incidents and crisis management

The supplier shall implement a procedure for processing incidents and crisis management in agreement with the operator.

This procedure describes the technical resources called upon in case of a crisis, such as applying a system configuration to avoid attacks or to limit their effect, forbidding the use of removable storage devices connected to the asset, or isolating the asset from the internet by physically or logically disconnecting the network interfaces.

The operator asks the supplier to put in place a full-time 24/7 service in case of critical incidents affecting the asset.

Such a full-time service may also be expressly requested by the operator to solicit the supplier's support for analysis of any incidents, vulnerabilities and threats affecting the security of the asset such as a search for markers that the assets has been compromised.

The operator asks the supplier to provide an operational security contact for the asset, and to put in place secure means of communication, approved by the operator, to be used during the crisis.

In case of a cyber-security incident, the analysis report and any related traces and evidence must be stored in a dedicated network with limited access on a need-to-know basis only.

Indicators

The operator assesses the security of its assets by monitoring indicators of maintenance in secure conditions, such as the percentage of users accessing the assets by type of account, the percentage of asset system resources not updated or corrected from a security point of view, etc.

The operator asks the supplier to provide support for establishing and producing the indicators stated in the rule (for example, the operator may ask the supplier to fill in a template it provides).

Asset access and administration

The supplier ensures the integrity of its own personnel and its service providers, particularly if the latter have extensive rights, and makes its personnel aware of security issues.

The operator wishes to identify the people, information systems and processes that have carried out an operation on the asset (this includes any consultation, addition, modification or deletion of a part of the asset). Which means for the supplier:

- that the operation and maintenance of the asset must be conducted only through named and not generic accounts, and that operations requiring highly privileged access must be carried out only via individual "administration accounts", and that when allocating rights, the principle of the strict minimum should be applied,
- that they must draw up and keep up to date the list of the named / individual accounts (administration and others) that they use, and that they renew the secret information of the named / individual accounts at least once per year,
- that they must deactivate and delete unused accounts,
- that they must document and justify any exceptions to these requirements, for example if it is not possible to create named / individual accounts for the asset,
- that they must apply the same directives to the subcontractors that operate or maintain the asset.

The process whereby a user accesses the asset or any similar automatic process relies on an authentication mechanism based on secret information.

The supplier shall provide the operator with the rules for managing the secret authentication information used for the asset:

- process for modifying the secret information, including by default, before commissioning the asset,
- process for renewing the secret information during the lifetime of the asset,
- mechanisms for protecting the secret information used in order to reduce access to such information to only those who need to know (encryption, access rights, different passwords for different privileged and unprivileged accounts),
- traceability measures that it is possible to implement in order to reduce the risk related to the use of secret authentication information, particularly if it cannot be renewed.

The supplier and its service providers shall only use administration workstations controlled by the supplier or by an agent duly authorised to operate and maintain the asset. These workstations shall be secured and disconnected from the internet or mail servers on the internet. These workstations must have antivirus software, encrypted storage memories, and be as up to date as necessary from a security point of view (operating systems, applications, etc.).

However, if for operational or organisational reasons, the supplier uses the workstation for operations other than administration, then they must put in place a firewall to separate the software environment used for these other operations from the software environment used for the administration operations. To do so, it is possible to implement remote access to an office environment from an administration environment, but not the other way around.

The administration workstations must be hosted on a network dedicated to system administration activities (privileged access to operator network assets), isolated from the rest of the supplier's IS. The workstation must preferably be used on business premises under the control of the supplier. If used outside such business premises, a remote access solution to the supplier's IS may be used and must ensure the integrity, authenticity and confidentiality of the flows (preferably IPsec encryption, TLS otherwise) and strong authentication for the administrator. The remote workstation must be configured so as to avoid constituting a gateway between the supplier's IS and any uncontrolled networks (e.g. internet).

If identification and authentication directories are used for the administration resources (administration workstations and tools used to operate or maintain the asset), they must be dedicated to these resources and deployed in trusted areas, reserved for administration resources.

All the service provider's technical tools used for the administration of the administration workstations (maintenance in secure and operational condition, configuration) must be dedicated to these resources and deployed in trusted areas, reserved for administration resources.

The supplier shall put in place strong authentication for all resources with access to the operator's IS in their environment that allows access to the hardware and / or software provided.

The administration flows for the asset shall be encrypted from the supplier's administration workstation, even if a VPN links the supplier to the operator. The operator expects the supplier to document and present the technical solution for the administration workstation out in place.

Installation, isolation and security

To limit the propagation of cyber-attacks, the supplier shall implement means of isolation (ACL, firewall) between the asset and its sub-systems regarding concomitant systems, in order to separate the different parts (user, data, control) of the asset. The input and output flows of the asset shall be documented in a matrix and reduced to the strict minimum. The same shall apply for the asset's internal flows, meaning between the different sub-systems.

The supplier shall implement mechanisms for securing the hardware and software comprising the asset. To do so, the supplier:

- shall list all the services active on the asset,
- deactivate the services and close the unused ports on the asset,
- install the latest levels of security patches and antivirus software on the asset before commissioning and propose an installation mechanism to update the security patches and antivirus software.

The operator may ask for the asset to be connected to its authentication, traceability, access (bastion) and antivirus platforms, its port and vulnerability scans, management patches and log management system. If, for operational reasons, the asset cannot be connected to such platforms, then the operator may ask the supplier to propose a plan to achieve compliance and the time necessary for its implementation.

The removable devices used by the supplier for asset integration, operation and maintenance operations shall be subject to an in-depth inspection prior to use to avoid, for example, the execution of any malware on the asset and may be notarised.

Technical requirements related to the GDPR

An asset that handles or stores personal data is subject to the General Data Protection Regulation (GDPR) as of May 2018, which means that the supplier of the asset must:

- propose to the operator a mechanism to pseudonymise the personal data collected without preventing the asset from functioning properly,
- propose to the operator a mechanism for returning the processed data after a pre-determined period. The data must not be re-identifiable,
- propose to the operator a mechanism making it possible to delete on demand data that are specific to one or more customers,
- propose to the operator a mechanism for extracting data on demand,
- propose to the operator a mechanism for excluding a subscriber from processing.