40 Essential measures for a healthy network

Agence nationale de la sécurité des systèmes d'information

Contents

FOREWORD

The formidable developments in IT and the Internet have revolutionised the way we live and work.

The loss or theft of certain information or the unavailability of a company's information system can have serious consequences for a company: loss of the trust placed in it by customers or partners, advantage being taken by a competitor, or operating loss caused by production downtime. The communications of the management team are often particularly targeted.

From now on, the safeguarding of confidential information passed on by customers and partners may provide a competitive advantage. Furthermore, protection of a company's data and IT network is crucial for its survival and competitiveness.

Although human error or the malicious acts of an employee may result in an incident, external hostile acts are becoming increasingly frequent: attacks on a company's website, malicious code (malware) concealed in email attachments or in captured USB sticks, password theft, etc.

Management has a duty to ensure that suitable protective measures are set in place and operational. These must be governed by a written security policy that all individuals are aware of and familiar with, and whose application must be regularly verified by supervisory management.

Among such measures are a number of simple technical measures, referred to as essential IT measures, being the translation into the digital world of basic healthcare rules.

The majority of IT attacks which have involved ANSSI stepping in could have been prevented had the IT measures set out in this guide been applied by the companies concerned.

This document has been written for persons tasked with IT security, be they Information Systems Security Managers (ISSM) or any other individuals discharging this role, and sets out 40 essential measures – that could be referred as rules - for a healthy network.

These measures are not intended to be exhaustive. However, they do constitute the minimum that must be followed to protect a company's information.

Failing to follow these measures places a company at risk of major incidents, which may jeopardise its competitiveness and even its long-term survival.

A MESSAGE TO THE IT MANAGERS

You are in charge of your organisation's information systems security or simply, you are the person responsible for the smooth operation of its IT systems. As you will be aware, in just a few years, your tasks have evolved with the arrival of new information technologies which now form the backbone of the operations of all businesses and national and local administrations, and also of our day-to-day lives. New uses are also making control over the systems with which you are entrusted ever more complex.

Customer databases, sales contracts, patents, production data, user files, administrative processes and information about public tenders are now accessible online, mostly through the Internet via computers or mobile phones.

The consequences for your organisation of the loss or theft of certain information or the unavailability of its IT system could be extremely serious. Conversely, the safeguarding of confidential company information or information passed on in confidence by customers, partners or suppliers inspires trust and helps activities to run smoothly.

Although human error or the malicious acts of an employee may sometimes be the cause of an incident, external hostile acts, for the purpose of espionage or even sabotage, are now extremely frequent and inconspicuous.

Nevertheless, numerous IT attacks, dealt with by the French Network and Information Security Agency (Agence nationale de sécurité des systèmes d'information or ANSSI), could have been prevented if crucial technical measures had been applied by the organisations that fell prey to these.

Some of these measures may be termed "basic IT rules". Failing to follow these will needlessly expose your organisation to the risk of major incidents, liable to jeopardise its operations or competitiveness, or even bring its activity to a standstill.

This guide has been written with you in mind. It sets out 40 essential IT measures to safeguard the security of your information system and explains how to implement them. Although they are not exhaustive, these rules nevertheless constitute the basic minimum that must be followed in order to protect the information of your organisation.

Once these rules have been shared and applied, you will have completed a significant part of your mission - that of enabling your organisation to interact with its suppliers and partners, and to serve its customers, whilst safeguarding the integrity and confidentiality of the information pertaining to them.

This document focuses on standard office systems. Although certain of the recommendations set out herein also apply to industrial systems, ANSSI has published a specific guide for safeguarding the security of these types of systems[1].

1 Please refer to the ANSSI website: www.ssi.gouv.fr/systemesindustriels.

I - KNOW THE INFORMATION SYSTEM AND ITS USERS

Knowing your information system is an important prerequisite to making it secure. In fact, if the information system includes equipment that is regularly omitted from inventories, this equipment will quickly become obsolete and will be a target of choice for an attacker.

Rule 1

Have an accurate map of IT installations and keep it updated.

Preparing a map of the information system is the first step in acquiring a more extensive knowledge of the information system. This will make it easier to devise safety measures that are adapted to suit the system, to ensure that no item of equipment is overlooked in applying a security measure and to facilitate a response in the event of an incident.

This map must at a minimum include the following elements:

- a list of equipment (stating model) and software (stating version) used. Obviously, this list needs to be as accurate as possible. As a starting point for this process, you may wish to create a list firstly of the machines used along with their appointees and technical parameters (IP address, MAC address), and secondly the main software packages used on these machines (office suite, PDF viewer, browser, email client) and their corresponding versions. Furthermore, administrator machines must be included in the equipment that is mapped. The more uniform the IT stock is, the easier it will be to create such a list and to keep it updated;
- the network architecture, identifying nerve centres (external connections[1], servers hosting sensitive data or operations, etc.).

Once this map has been created, it can be updated and elaborated upon, particularly with the elements relating to protocols implemented (flow matrices).

1 **Specifically, conduct an inventory of all Internet access points for the information system and all interconnections with partner networks (suppliers, sales partners, etc.). This inventory must be exhaustive. It must include any ADSL access points that may have been created for specific user requirements and specialist connections.**

This map must not be stored on the network that it represents, since this is one of the elements that a hacker will look for first of all in the event of a successful intrusion.

Keep an exhaustive inventory of privileged accounts and ensure this is updated.

At a minimum, it is important to have a list of:

- Users with an administrator account (or with privileges higher than those of a standard user) on the information system;
- Users with sufficient privileges to access to the work directories of managers or, particularly, of all users;
- Users with a machine that is not administered by the IT department and therefore not managed in accordance with the organisation's general security policy.

This list must be kept updated.

It is also important to have a list of users with sufficient privileges to read the emails of company management or particularly of all users. However, compiling a list of the individuals that actually have access to this information can sometimes be extremely difficult. If such a list cannot be reliably compiled, a mailbox access log would need to be created and the list of individuals consulting the most sensitive mailboxes periodically verified (see rule 26).

In a Windows system, most of this information may be obtained by analysing the configuration of the Active Directory. The document entitled *Audit des permissions en environnement Active Directory*[2] (*Auditing permissions in an Active Directory environment*) , available on the ANSSI website, sets out a number of methods for conducting an inventory.

It is also very highly recommended that you use a clear nomenclature for account names (service accounts systematically preceded by the prefix SRV, administrator accounts by the prefix ADM).

2 Please refer to http://www.ssi.gouv.fr/Active-Directory.

Rule 3

Create and apply procedures for the arrival and departure of users (personnel, interns, etc.).

These procedures are intended to ensure that the rights granted on the information system are applied as judiciously as possible. It is particularly important that all rights allocated to an individual are revoked when they leave. The procedures must at a minimum set out:

- management (creation/deletion) of IT accounts (and their corresponding mailboxes) and allocation of the rights associated with these accounts on the information system including for external partners and service providers;
- management of access to premises (in particular, the receipt and return of swipe cards to the premises);
- management of portable machines;
- management of sensitive documents (possession, any authorisations for removal from the premises);
- management of the control of personnel authorisations.

It is important that changes of personnel are properly managed, either by treating this as a departure followed by a new arrival or by defining a suitable procedure. The privileges associated with certain user accounts often increase with internal movements, which result in the allocation of new rights without deleting those that no longer apply.

II - CONTROL THE NETWORK

Rule 4

Limit the number of Internet access points for the company to those that are strictly necessary.

You should be able to precisely identify Internet access points (ADSL box, etc.) and interconnections with partner networks and should limit these to the minimum strictly necessary to make it easier to centralise and standardise the monitoring of traffic.

Rule 5

Prohibit the connection of personal devices to the organisation's information system.

The connection of personal devices may only be permitted on networks containing absolutely no sensitive information. Personal devices (PDAs, tablets, smartphones, MP3 players, USB sticks) are actually difficult for an organisation to control in the sense that the users themselves determine the level of security for their devices. The security measures in place in an organisation or company, therefore, cannot, by their very nature, be applied to these types of devices.

This rule is frequently perceived as an unacceptable and even retrograde restriction by a great number of users. However, unless this is adhered to, the task of a hacker is made very much easier by making a company's network vulnerable. In fact, for every one hundred personal devices connected to a company's network, it has been statistically estimated that at least ten of these have been compromised by generic malware (leaving aside targeted attacks).

It is therefore important to prohibit or prevent their connection to a company's information system. This prohibition should apply first and foremost at the organisational level: even if there are no technical rules preventing their connection, users should be encouraged not to adopt such practices, for example through the charter governing the use of IT resources.

To the greatest extent possible, this prohibition must be supplemented by technical measures, which can however sometimes prove more complex to implement (systematic control of network access, deactivation of USB ports).

Where there is a need to work remotely, the organisation must provide the professional means to enable this type of use. The transfer of emails from professional to personal mailboxes, however, must be explicitly prohibited.

III - UPGRADE SOFTWARE

On a daily basis, vulnerabilities are revealed in a large number of widely used software packages. Sometimes just a few hours are enough for malware exploiting these vulnerabilities to begin to circulate on the Internet. It is therefore very important to prioritise the use of established technologies, for which support is guaranteed, to avoid technologies that your in-house team is not totally competent in, and to follow the recommendations of this chapter.

Rule 6

Know how all software components are updated and keep up-to-date on the vulnerabilities of these components and their required updates.

II It is crucial to determine how software components used by the company can be updated. If a software component cannot be updated, it must not be used (see rule 7 for how to manage exceptions in this regard). Also, updates (like software) must only be downloaded from trusted sites (the site of their publisher, generally).

We recommend dealing with core components as a priority (operating system, office suite, browser and browser tools – such as Java virtual machine or Flash player, document viewers) and then supplement the inventory with all other software components and add these items to the map.

You will also need to carry out an inventory of and monitor sources of information liable to pass on vulnerabilities to the identified components and disseminate updates (website of publishers of the software in question, CERT websites).

Rule 7

Define and strictly apply an update policy.

This policy must include:

- Items to be updated;
- the responsibilities of the various actors in the updating process;
- the means used to obtain and assess updates.

This may take the form of a simple table containing these points.

L A dedicated tool should be used, if one exists (for example WSUS for Microsoft environments) enabling updates to be applied uniformly across the entire IT stock. Generally speaking, an assessment of updates in terms of their impact on system function must be carried out prior to application.

In the light of rule 6 above, it is vital that no components, and particularly no machines, be excluded from the update policy.

Unfortunately, however, IT departments frequently keep an obsolete system running that is no longer supported by its manufacturer because certain applications are particularly well-suited to that system. In this case it is vital that such systems be isolated:

- at the network level, using a very strict filter that only authorises access to the necessary applications;
- at the authentication level, ensuring that no passwords (either for the system or for software) are shared with the rest of the information system;
- at the application level, by ensuring that these systems do not use resources shared with the rest of the information system.

Furthermore, isolated devices (disconnected from the network) must not be left out of the update policy. Manual updating is essential for these systems.

IV - AUTHENTICATE THE USER

Passwords are often the Achilles' heel of information systems. In fact, although organisations quite often formulate a password policy, only rarely is this uniformly applied across the entire IT stock.

Identify each individual accessing the system by name.

This rule is intended to eliminate generic and anonymous accounts and access and designed to make it easier to attribute an action on the system to a specific individual. This is especially useful in the event of an incident.

Of course, this rule does not stop you from retaining technical accounts (termed service accounts) that are not attributed to a specific individual but rather to a department, a business unit or an application (for example an "apache" user for a web server). However, these accounts must be managed with a policy that is at least as stringent as the one for named user accounts.

Set rules for the choice and size of passwords.

Good practice for the choice and size of passwords may be found in the ANSSI document entitled Recommandations de sécurité relatives aux mots de passe (Security recommendations for passwords)[3]. Of these rules, most critical are to make users aware of the risks involved in choosing a password that is too easy to guess, and the risks of reusing the same password, especially for personal and professional mailboxes.

3 Please refer to http://www.ssi.gouv.fr/mots-de-passe/.

Rule 10

Set in place technical methods to enable authentication rules to be followed.

The following methods enable authentication and password rules to be followed:

- blocking of accounts every 6 months until the password has been changed;
- blocking of any configuration of a machine that permits start-up in "autologon" mode (i.e. without a password) or from a guest account;
- verifying that the chosen passwords are not easy to work out.

Some tools have the native ability to verify when a password is changed that the new password chosen is not too easy to work out using the old password. Although the intention of this kind of tool may be commendable (it is indeed often easy to guess a user's new password if their other passwords are known), it is strongly recommended that you do not use these unless you are fully competent in their use as they can require that a history of previous passwords be stored.

Rule 11

Do not store passwords in plain sight in files on information systems.

To keep things simple, users and administrators often write their passwords in plain sight in files stored on their computers or send them to themselves via email. These practices must not be permitted. Passwords and secret information stored on users' machines are the first thing that hackers will look for and use.

It is also important not to use automatic password storage mechanisms (for example, the "always remember password" button of a browser). If the number of passwords makes use of a centralised storage solution necessary, a system whose security has been validated must be used. ANSSI has certified products that permit this type of use[4].

4 http://www.ssi.gouv.fr/fr/produits-et-prestataires/.

Rule 12

Systematically renew default authentication settings (password, certificates) on devices (network switches, routers, servers, printers).

Default settings are systematically known by attackers. Also, they are very frequently trivial (password the same as username, password shared by several devices in the same range, etc.). They must therefore be changed. If it is not possible to change them (certificate "hardwired" into a device, for example), this critical issue must be made known to the manufacturer so that they can correct this vulnerability as expeditiously as possible.

Rule 13

Opt, where possible, for strong, smart card authentication.

We highly recommend setting in place strong authentication based on the use of a smart card requiring a PIN code (please refer to annex B.3 of the General Security Mechanism[5]).

Implementing a chip-and-pin-based access control mechanism in a system, which doesn't have one, however, is a lengthier and more costly exercise than implementing the other rules set out in this document.

5 http://www.ssi.gouv.fr/rgs/.

V - SECURE COMPUTER TERMINALS

Although up until a few years ago, hackers targeted servers before anything else, one of the easiest ways of penetrating a network today is by hacking a client machine. Not infrequently client machines are actually less secure and above all less well supervised than servers.

Implement a uniform level of security across the entire IT stock.

Specifically, at a minimum, it is vital to deactivate unnecessary services and restrict user account privileges. The use of a personal firewall on each client machine, configured at a minimum to block unsolicited incoming connections, is generally speaking indispensable. Where systems allow, for example on client servers or machines running Linux, hardening of the operating system through the addition of optional security components such as GRSec and PaX should be considered.

Additionally, the BIOS of machines must be locked with a non-trivial password and start-up on removable media or via the network (Wake On LAN) must be deactivated.

At the applications level, the following should be configured as meticulously as possible: incoming email clients (forcing the sending and receipt of emails in plain text rather than HTML is a good practice for example), browsers (default blocking of certain content and only activating that media on a case-by-case basis, for example), or office suites (deactivate the ability to run macros).

Regarding this last point, it should be noted that although the blocking of certain content, such as JavaScript and Flash, is essential from a security point of view, it is often perceived to be difficult or even impossible since these technologies are required to access the information. It is nevertheless important that these technologies are, at the very least, deactivated on machines where their use is not strictly necessary.

Rule 15

Technically prevent the connection of portable media except where strictly necessary; deactivate the execution of the autorun functions from these types of media.

Portable media are a preferred method for the propagation of malware and data exfiltration. Their usage should therefore be kept to a minimum. Often it is unrealistic to completely prevent the connection of portable media on company machines. The right approach is to identify those machines for which the connection of portable media is required, and to authorise connection to these alone and update this list frequently so as to minimise the number of machines included on it.

A number of organisations prefer to opt for the use of clean machines (or "access locks") that all portable media must go through before being connected to the company system. Although the intention is commendable (checking that media pose no threat before connecting them), these machines rapidly become one of the nerve centres of the information system (they are accessible to all users, and they are themselves highly exposed). They should only be used if they can be completely controlled.

In any event, the automated running of code from portable media (*autorun*) must systematically be technically prevented.

Moreover, on Microsoft systems from Windows XP onwards, it is possible to restrict the ability to run programs using several criteria, through the Software Restriction Policies. Such a policy may be set in place in order to limit the risk of accidentally importing a virus, especially through a USB key.

Rule 16

Use an IT stock management tool that enables the deployment of security policies and updates to machines.

Using an IT stock management tool is vital in order ensure that machines on the network are monitored.

You will need to include the greatest possible number of IT machines within those that are managed by the tool in question.

Rule 17

Manage portable machines with a security policy that is at least as stringent as for fixed machines.

If there is any difference in the way fixed and portable machines are managed, the actual security level of the network will be that of the weakest link.

Portable machines will need to be managed using at least the same security measures as fixed machines (updating, restriction of privileges, etc.). The conditions under which portable computers are used often make it also necessary to enhance certain security functions (disc encryption, enhanced authentication, see rule 19) but the implementation of such functions on fixed machines is also a good practice for defence in depth.

Rule 18

Wherever possible, prohibit remote connections to client machines.

In cases where the application of this rule is not possible, you must adhere strictly to the principals set out in the technical document entitled *Recommandations de sécurité relatives à la téléassistance*[6] (*Security recommendations for remote assistance*).

Rule 19

Encrypt sensitive data, especially on mobile machines and media that may get lost.

The loss or theft of a mobile device or portable machine (or media) may have serious consequences for the company: unless encrypted, the data stored on the machine (technological assets of the company, customer database) will in effect be compromised, even where the machine is switched off or the user session terminated. For this reason, it is important to encrypt sensitive data. A number of disk or partition encryption systems (or encrypting media) have been validated by ANSSI[7]. Priority should be given to their use. ANSSI validation guarantees the strength of the encryption mechanisms used.

Encryption can be carried out system-wide (known as full system encryption), on a sub-section of the system (partition encryption) or on the most sensitive files. Full disk encryption mechanisms are the most effective from the point of view of security and do not require the user to identify the files to be encrypted. In cases where implementation of this type of system encryption proves too complex (for example, a small organisation), it is essential to provide users with a partition encryption system.

6 Please refer to http://www.ssi.gouv.fr/IMG/pdf/NP_Teleassistance_NoteTech.pdf.
7 Please refer to http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/ .

VI - SECURE THE INSIDE OF THE NETWORK

It is important not merely to implement perimeter measures, such as firewalls and proxy servers. Indeed, although these are indispensable (see Section VII), there are a number of ways these can be circumvented by hackers. Consequently, it is vital for the network to be protected against a hacker who has already breached such perimeter defence measures.

Directory Services (*Active Directory, Lightweight Directory Access Protocol* - LDAP) enable each user to be allocated rights over an information system and are also crucial elements that are ripe for targeting by hackers and whose integrity must frequently be verified.

Frequently audit (or have audited) the configuration of the central directory (*Active Directory* in Windows environments or LDAP directory for example)

We recommend following the rules set out in the article entitled *Auditing permissions in an Active Directory environment*[8]. In particular, you should verify at regular intervals that the access rights to the data of key individuals within the company (particularly managers) are correctly set.

8 Please refer to http://www.ssi.gouv.fr/Active-Directory.

Rule 21

Set in place compartmentalised networks. For machines or servers containing information that is of strategic importance to the company, create a sub-network protected by a specific interconnection gateway.

With a flat network[9], the compromising of a domain controller will systematically result in the entire network being compromised.

It is important to take this rule into account ahead of time when the network is being designed. In fact, depending on the extent of the network and its complexity, it will frequently be very difficult to compartmentalise the network at a later stage. We recommend in networks that it would not be straightforward to compartmentalise:

- taking into account compartmentalisation requirements in any further extension of the network;
- engaging in strategic thinking regarding the network architecture which, strictly speaking, falls outside the scope.

Rule 22

Avoid the use of wireless (Wifi) infrastructures. If the use of these technologies cannot be avoided, compartmentalise the Wifi access network from the rest of the information system.

The use of wireless technologies within the network is not recommended (limited guarantee of availability, difficulty of designing a low cost secure access architecture, etc.).

If such technologies must be used, network architecture segmentation must be able to limit the consequences of intrusion via radio access up to a given perimeter. Compartmentalisation of the wireless access network from the rest of the network is highly recommended: interconnection with the main network must be through a controlled gateway allowing the tracking of access and the restriction of traffic to

9 A "flat" network is a network with no internal network compartmentalisation mechanism. It is therefore possible for each machine on the network to access any other machine on the network

necessary flows alone. The design of this type of access network falls outside the scope of basic IT measures.

Furthermore, it is important to give priority to the use of Wifi network encryption that is based on WPA Enterprise (EAP-TLS with WPA2 CCMP encryption) which enables machines to be authenticated by means of client certificates from machines accessing the network. Protection mechanisms based on a shared key must be prohibited where external service providers or an excessive number of users have to be required to access this Wifi network.

You should also avoid using PLC (PowerLine Communication) technologies without using protection mechanisms equivalent to those recommended for wireless technologies. Indeed, the perimeter covered by the PLC network is difficult to accurately determine.

Rule 23

Systematically use secure applications and protocols.

The use of secure protocols, including on the internal network, contributes to defence in depth and complicates the task of a hacker who has already compromised one machine on a network and who seeks to extend their control over that network.

Insecure protocols (telnet, FTP, POP, SMTP, HTTP) are, as a general rule, not to be permitted on a company network, and should be replaced by their secure equivalents (SSH, SFTP, POPS, SMTPS, HTTPS, etc.).

Furthermore, it is important that business applications are developed taking into account security risks. Their required use of a specific technology (typically a given version of an operating system or Java virtual machine) must be restricted, so as not to limit the ability of these applications to be maintained under secure conditions and updated.

VII - PROTECT THE INTERNAL NETWORK FROM THE INTERNET

Although certain attacks may be internal in origin, one of the principal means of attack encountered by ANSSI is infection following connection to a compromised website. In addition to protection measures for the internal network, such as limiting the number of interconnections, as set out earlier in this document, it is therefore important to implement specific perimeter defence measures.

Secure Internet interconnection gateways.

This will require the setting in place of correctly configured security services (i.e. compliant with the recommendations of the document entitled *Définition d'une architecture de passerelle d'interconnexion sécurisée*[10] (*Definition of a secure interconnection gateway architecture*) enabling compartmentalisation between Internet access, the service area (DMZ) and the internal network.

Ensure that there are no machines on the network with an administration interface that is accessible via the Internet.

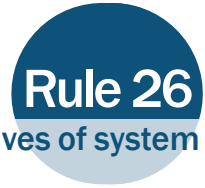
Many machines have administration interfaces (for example via a web server). Some of these interfaces have default access and consequently are only deactivated when explicit action is taken by the machine's administrator. These interfaces are often exploited by hackers during an intrusion, especially if these are exposed on the Internet. Several thousand companies expose this type of interface on the Internet, often without even realising.

This rule applies to printers, servers, routers, network switches and industrial or monitoring machines.

10 Please refer to http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/definition-d-une-architecture-de-passerelle-d-interconnexion-securisee.html.

VIII - MONITOR SYSTEMS

The majority of the measures covered thus far have been preventive in nature and intended to reduce the risk of exploitation of system vulnerabilities by a hacker. The setting in place of preventive measures can never be a substitute for system monitoring during its operation. Monitoring must follow the rules set out in this chapter.



Clearly define the objectives of system and network monitoring.

In the majority of cases, the following events must generate an alert, which must imperatively be dealt with within 24 hours:

- connection by a user outside normal working hours or during a stated period of absence;
- very substantial transfer of data outside the company;
- successive or repeated attempts to connect to a service;
- connection attempts from an inactive account;
- attempts to circumvent the security policy (use of a prohibited service, unauthorised connection to a service, etc.).

Define event log analysis methods.

It is also crucial to define log verification procedures that will enable an alert to be generated as soon as one of the designated objectives is not fulfilled. These procedures must ensure that logs are frequently analysed.

In addition to the points referred to in rule 26, log analysis may be focused on the following in particular:

- analysis of the access list to the mailboxes of key persons within the company;
- analysis of access to sensitive company machines or resources.
- To facilitate log checking, it is vital for machines' clocks to be synchronised.

IX - SECURE NETWORK ADMINISTRATION

In a number of cases dealt with by ANSSI, hackers have, via the Internet, taken complete control of administrator machines or administration accounts in order to obtain the highest system privileges.

Rule 28

Prohibit all access to the Internet from administration accounts.

This prohibition applies particularly to system administrator machines. This rule is generally received unfavourably by users as it may create operating restrictions (having to use separate accounts depending on what actions are being taken). The burden of this restriction can be made considerably lighter, for example by providing administrators with two separate machines, so that they can consult documentation on a manufacturer's website with one machine (using their non-privileged account) whilst administering the machine in question on the other (using their administrator account). This will also make rule 29 easier to apply.

Rule 29

Use a dedicated network for the administration of machines or at least a network that is logically separated from the user network.

It is necessary to compartmentalise the administration network from the users' work network. We recommend (based on the capabilities of the organisation):

- prioritising physical network compartmentalisation wherever possible;
- failing this, setting in place logical cryptographic compartmentalisation based on the implementation of IPsec tunnels that use a product validated by ANSSI. The integrity and confidentiality of information transported across the administration network is therefore kept secure from the company's ordinary work network;
- at a minimum, implement logical compartmentalisation using VLAN.

Because administration accounts are particularly critical, priority must be given to monitoring of these networks. It is vital that machines on the administration network be kept updated.

Rule 30

Do not grant administration privileges to users. Make no exceptions.

Many users, even at the top of hierarchies, are tempted to ask their IT department to be granted greater privileges over their machines (ability to install software, ability to connect personal devices, etc.). This type of use is far too dangerous, however, and is liable to jeopardise the entire network.

Rule 31

Only authorise remote access to the company network, even for network administration, from company machines that use strong authentication mechanisms and protect the integrity and confidentiality of traffic using robust means.

To do so, give priority to the use of authentication mechanisms and integrity and confidentiality protection methods that have been validated by ANSSI.

X - CONTROL ACCESS TO THE PREMISES AND PHYSICAL SECURITY

Security of the system controlling access to the premises is often critical to a company's security. Indeed, as soon as a hacker succeeds in accessing the company's internal network, the perimeter security measures implemented become ineffectual. The bringing into line of physical security measures with the protection requirements for information systems is further complicated by the fact that separate teams are frequently in charge of these two areas. The responsibilities of each team must be clearly and formally set out.

Robust control mechanisms for premises access must imperatively be used.

The access control mechanism set in place must be state-of-the-art to ensure that it cannot easily be circumvented by a hacker. ANSSI has published a guide to assist companies in selecting robust access control mechanisms[11].

Keys to access the premises and alarm codes must be scrupulously protected.

The following rules must be applied:

- always take back an employee's keys or badges when they leave the company permanently;
- change company alarm codes frequently;
- never give keys or alarm codes to external providers unless it is possible to track their access and technically restrict this to given time intervals.

11 Please refer to http://www.ssi.gouv.fr/sans-contact.

Rule 34

Do not leave access sockets to the internal network accessible in locations that are open to the public.

These public locations may be waiting rooms, cupboards or corridors, for example. Hackers may, for example, be able to gain access to the company network by connecting a hacking computer in the place of the following types of equipment, where these are connected to the network:

- multi-function printers or photocopiers located in a corridor;
- monitors displaying information flows;
- surveillance cameras;
- telephones:
- network sockets in a waiting room.

Neither should internal network cabling be accessible in public locations.

However, if there are occasions when the network needs to be made available from a socket located in a public space (for a presentation for example), the socket must be made available for the occasion and removed as quickly as possible thereafter.

Define rules for the use of printers and photocopiers.

The following rules may be defined:

- use printers with a mechanism that requires the physical presence of the user in order to start printing;
- at the end of the day, destroy any documents left on the printer or photocopier;
- shred documents rather than putting them in the waste paper basket.

Similarly, it is advisable to implement clear procedures for the destruction or recycling of IT media at the end of their useful lives.

XI - ORGANISE RESPONSE IN THE EVENT OF AN INCIDENT

When it is discovered that machine has been compromised (e.g. a computer infected by a virus), you will need to determine quickly, although without excessive haste, a course of action enabling the potential seriousness of the incident to be determined in order to take the appropriate technical, organisational and legal measures, to contain the infection and quarantine compromised machines. It is important to think before acting so as not to take hasty decisions that could have detrimental consequences.

Develop a plan for IT recovery and continuity of activity, even if only in outline, that is regularly updated, setting out how to safeguard the company's essential data.

It is vital for a company to have a plan for IT recovery and continuity of activity, ideally including an area focusing on response in the event of an IT attack.

Analysing the consequences for the company's activity of certain disasters can be a good starting point: what would happen if access to the Internet were down for two days? What would happen if a hacker erased all of the data stored on the servers?

The company's sensitive data must periodically be backed up. Preferably, this back-up will be automatically to file servers and not be dependent solely on the good intentions of users who are frequently liable not to take the time to carry out such back-ups. Backups must periodically be checked and ideally should be stored in a separate location from where the operational servers are located.

Rule 37

Implement an alert and reaction chain that all parties involved are familiar with.

At a minimum, all users must be able to quickly contact a designated point of contact, with response training, to notify them of an incident. They must be able to get hold of this point of contact easily and must be informed that it is not advisable for them to attempt to deal with the issue singlehandedly.

Where the size of the company permits and whenever the stakes justify this, it is advisable for the alert chain to include an on-call or even a 24-hour component so as to ensure that detected incidents can be dealt with as effectively as possible.

Rule 38

Never simply deal with the infection of a machine without attempting to establish how the malware came to be installed on that machine, whether it has spread elsewhere on the network and what data has been accessed.

Many companies, in not going on to determine the full extent of an infection, have wasted many weeks, and even months, dealing with an incident. Each time an incident is dealt with, it must be the object of feedback and be capitalised upon in order to be more effective in dealing with a similar event in the future.

The following are examples of questions that you should ask:

- what type of machine was compromised? Do we have any others of the same type that are exposed to the same threats on the network?
- what data is the hacker liable to have had access to?
- was the compromised machine in communication with other machines or servers?

In the event of a machine being compromised, to make the work of investigating teams easier, those in charge may take the following measures:

- isolate infected machines from the network (unplug the network cable);
- do not power off infected machines in order to keep information relating to the malware available in the memory;
- copy or have specialists make copies of the memories and hard drives of the infected machines in order to carry out investigations. Check the integrity of copies prior to any operations involving updating, alteration of configuration, attempted cleaning or re-installation on compromised machines;
- fully reinstall the machine after disk copying if it is required to be returned to service. Never simply perform a restore or "cleaning" operation, which few experts would be able to perform.

XII - RAISE AWARENESS

Make users aware of the basic IT rules.

Each user should always (at least annually) be reminded:

- that the information they handle must be treated as sensitive;
- that the security of this information depends, in part, on acting in an exemplary manner in this regard and following the basic IT rules (not circumventing the security policy, always locking sessions when users leave their work station, not connecting personal devices to the company network, not disclosing passwords to third parties, not reusing professional passwords in a personal context, providing notification of suspicious events, accompanying visitors and external consultants, etc.).

Following the IT rules that concern users should form part of a user charter for the IT resources made use of by each user.

XIII - CARRY OUT A SECURITY AUDIT

Periodically carry out a security audit (at least annually). Each audit must be accompanied by an action plan, the implementation of which should be monitored at the highest level.

The carrying out of technical audits on an IT system is essential. Indeed, an audit is the only effective means of being completely certain of the efficacy of measures implemented on the ground. Each audit will provide an opportunity for a corrective action plan to be implemented. Monitoring meetings for this action plan will need to be organised frequently. For greater efficiency, progress on the action plan will need to be summarised in a dashboard indicator for the highest echelons of management.

INDEX

NOTES

Version 1.0 - January 2013
20130820-1440

Agence nationale de la sécurité des systèmes d'information

ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Websites : www.ssi.gouv.fr and www.securite-informatique.gouv.fr
Email : communication@ssi.gouv.fr