Guide to Information Technology Security

WMO-No. 1115

World
Meteorological
Organization
Weather • Climate • Water

WMO-No. 1115

Chair, Publications Board
World Meteorological Organization (WMO)
7 bis, avenue de la Paix
P.O. Box 2300
CH-1211 Geneva 2, Switzerland

Tel.: +41 (0) 22 730 84 03
Fax: +41 (0) 22 730 80 40
E-mail: publications@wmo.int

ISBN 978-92-63-11115-9

NOTE

The designations employed in WMO publications and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of WMO concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Opinions expressed in WMO publications are those of the authors and do not necessarily reflect those of WMO. The mention of specific companies or products does not imply that they are endorsed or recommended by WMO in preference to others of a similar nature which are not mentioned or advertised.

Revision History

2005-02-02 – ET-EUDCS, Draft version.
2006-07-19 – ET-CTS, First complete version.
2012-04-18 – ET-CTS, Second version with review of all text and addition of external references.
2016-04 – ET-CTS, Document review.

CONTENTS

1 INTRODUCTION

The quality of scientific work, research and services supporting the health and safety of humans depends on the exchange of meteorological and environmental data and on discussions that occur within the World Meteorological Organization (WMO) community.

Communication is essential for achieving business goals, and the Internet is one of the essential tools for exchange of information. Electronic means to transfer files, such as e-mail, the World Wide Web and social networks, have allowed the development of cooperation among scientists and improvements in the forecast and distribution of elaborate meteorological products.

However, in parallel to these positive changes in the way the WMO community works, an increasing number of threats are prevalent throughout the Internet, and it is necessary for organizations to face the dangers and protect information systems in order to maintain operational data processing and communication.

The Internet is a network of networks. It offers distributed services such as the World Wide Web that allow the browsing of information located on servers around the world, exchange of e-mail, exchange of files and much more. Owing to its widespread presence and use, the Internet has also unfortunately become a medium of choice for disseminating unwanted information and for launching electronic attacks against organizations and their information assets. The problem has become widespread and unavoidable.

For example, it would potentially only take minutes for a newly purchased computer system to become infected with some form of electronic virus if it was connected to the Internet without adding any security measures. The risk is high, as there are many electronic viruses, worms, directed attacks, pirating events, etc.

Furthermore, because centres are interconnected, they all have a responsibility to secure themselves to ensure they will not be the cause of further security problems with partners. Centres are only as secure as the least-secure centre in the network. Therefore, the threat must be dealt with.

For information about top security risks and methods to prevent or mitigate them, please refer to appropriate links, such as http://www.sans.org/top-cyber-security-risks/.

The purpose of this publication is to provide the reader with a broad overview of the main information technology security (ITS) components and procedures. It is not meant to be an extensive security course, as such information is widely available in the information technology (IT) industry. It is aimed at high-level managers, system managers and technicians who wish to have an introduction to ITS. It should act as an aid to understanding the basic concepts and principles of ITS, and help the reader to direct further study in this ever-widening field of computer science.

In very general terms, ITS can be achieved by:

- Establishing adequate security policies and ensuring all staff in an organization are well trained on their meaning.
- Establishing adequate security procedures to ensure that there is a regular systematic approach to all ITS matters.
- Building a zoned network architecture that will provide resilience against attempts to compromise systems, networks and hosts. In this context, a zone is a logical area within a networking environment with a defined level of network security.
- Monitoring external connections in order to detect any abnormal access or activity.

- Regularly applying security patches to critical systems as they become available.
- Ensuring that access control mechanisms are in place, commensurate with the system being protected, and managing them with diligence.
- Reinforcing best security and cultural practices across organizations through continual security education.

A complete list as defined in the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) information security standard 27002 can be found at http://en.wikipedia.org/wiki/ISO/IEC_27002.

2 INFORMATION TECHNOLOGY SECURITY

The purpose of ITS is to help an organization fulfil its mission by protecting its IT resources, which also include observation systems, and, through that, its assets.

Adequate security requirements can be defined using the following steps:

- Identify the assets;
- Identify the proper security criteria with, for each criterion, a proper scale (see section 2.3);
- Identify the asset security needs, according to the defined criteria;
- Conduct a risk analysis (some risks are listed in section 2.2);
- Identify the security techniques and procedures to consider (see section 2.4).

Additional information regarding information security standards can be found at http://en.wikipedia.org/wiki/ISO/IEC_27002 and http://en.wikipedia.org/wiki/ISO/IEC_27001, and in section 5 below.

The next four sections briefly mention some of the tasks necessary to implement ITS. This is not a complete list, and should always be complemented by tasks from the above-mentioned standards.

2.1 Protecting systems against potential failures

All IT resources play a part, which must be correctly understood, in permitting an organization to deliver services according to its mission. Any failure in these IT resources can then affect the capability to deliver these services.

Moreover, some organizations have dedicated links with partners. By default, these partner links should be considered similarly to any other public link (such as a connection to the Internet). They could be used to propagate security threats.

Thus, ITS is concerned with establishing policies, architecture and procedures so that the operation of these IT resources mitigates the potential failures and their impacts, thus maintaining a high level of service and minimal impact to other partners and clients.

2.2 Malicious versus non-malicious activities

ITS must be concerned with malicious and non-malicious activities. Both can be a cause of trouble. For example, malicious activities can include fraud and theft, internal or external hackers, and malicious codes such as viruses, spyware or espionage. Non-malicious activities can include errors, omissions, and loss of physical and infrastructure support.

2.3 Establishing security criteria

Security criteria allow an organization to evaluate the risks that may affect a given asset. Three security criteria are considered in most cases:

- Availability: When or how often an asset must be present or ready for use;
- Integrity: The authenticity, accuracy and completeness of an asset;
- Confidentiality: The need to keep proprietary, sensitive or personal information private and inaccessible to anyone who is not authorized to see it.

Other security criteria can also be taken into account, such as accountability, auditability, anonymity and reliability.

In all cases, these criteria are chosen by each organization, thus specifying the level of security required for specific IT components.

2.4 Security techniques and procedures to consider

Once an organization has properly identified its ITS requirements, measures should be implemented to technically and procedurally deliver against those requirements.

Monitoring and reporting should give the organization some visibility of its information system. They must be defined so that a security incident can be detected, its origin identified and for this to act as an enabler to a complementary process that would limit the threat boundary (such that it is prevented from doing further damage to connected systems/data).

Predefined incident handling and disaster recovery procedures are helpful in minimizing the impact of an ITS-linked event within an organization, by reacting quickly and in a proper manner to the incident, and by being able to recover the essential elements affected.

Once the incident is over, it must be analysed so that potential lessons can be learned.

3 SECURITY THREATS

3.1 Reasons for threats

Motives for threats can be deliberate or accidental, as outlined below.

3.1.1 Obtain information or resources

An attack can be motivated by the will to obtain information, for strategic, ideological, financial or intelligence reasons, or resources such as storage, supercomputing or a link to an organization’s partner.

3.1.2 Desire to cause harm

Another motive can be to prevent an organization fulfilling its mission properly, by blocking or modifying services or information, for revenge, terrorism, blackmail or malicious reasons.

3.1.3 Playful or exploration

Another kind of motive is curiosity, boredom, game or challenge. Many famous governmental institutions have been affected by such attacks, degrading their reputation.

3.1.4 Accident

The last category is human or physical accident or oversight. This can take many forms and touch any part of the information system (network, hardware, software or procedural), and can be mitigated by adequate procedures and training, such as by implementing system redundancy and automatic failover procedures, being aware of public visibility or delivering regular training.

3.2 Common threats

A useful link for this topic is https://www.sans.org/critical-security-controls.

3.2.1 Malicious codes: viruses, ransomware, worms and Trojans

A virus is a destructive computer program that spreads from computer to computer using a range of methods, including infecting portable storage (for example, Universal Serial Bus (USB)), infected web pages and other programs. Viruses often attach themselves to a program and modify it so that the virus code runs when the program is first started. The infected program typically appears to run normally, but the virus code then infects other programs whenever it can.

A worm is a special type of virus that does not attach itself to programs, but rather spreads via other methods such as e-mail.

A Trojan (or backdoor) is a program that performs the desired task, but also includes unexpected functions, such as allowing remote connection to the infected computer or sending information.

All these codes have the potential to disrupt services, destroy information, use resources for their own good or any other function that the originator of the code may wish to implement.

3.2.2 Denial of service

A denial-of-service attack is characterized by an attempt to prevent legitimate users of a service from using that service. These attacks can be deliberate or accidental, such as abusive use of storage, network and supercomputing resources. They can also be from distributed (and therefore difficult-to-block) sources, using networks of compromised hosts called “botnets”.

3.2.3 Malicious hacking

Malicious hacking refers to breaking into IT resources without authorization.

3.2.4 Spying

Spying is the act of gathering proprietary data from the organization for the purpose of aiding another company or government. It can concern personal information, confidential data and proprietary software.

3.2.5 Compromising and abusing system resources

Compromising and abusing system resources can be deliberate (hacker) or accidental (side effect of a legitimate user action). These include the ability to modify codes and data, and to use supercomputing, storage and network resources. They can also lead to a denial of service, even if it is not the primary goal.

3.3 Main attack methods

An attack method is a way for a threat agent to launch an attack.

3.3.1 Hacking systems by finding security holes in systems

The computers that comprise IT systems contain complex operating systems and various software modules. By their very nature, these systems offer many configuration options, features and potential deficiencies. All these components, if not kept up to date regarding security holes, or if not properly configured, can easily be used by a threat agent (human, such as malicious hackers, or non-human, such as viruses) to compromise the system. If the security hole is not known to the vendor, it is termed a zero-day vulnerability. Patches should be applied when they become available.

Specific tools exist, used by security staff as well as malicious hackers, to identify both security holes and configuration weaknesses on a system.

3.3.2 Denial-of-service attacks

These attacks can either be caused by exploiting security holes in systems, or simply by directing masses of traffic towards a particular system. In both cases, the system is rendered almost unusable because of the overload, thus blocking access to servers, sites and even the Internet.

Improper configuration or weak operating systems are also vulnerable to such kinds of attacks.

3.3.3 Malicious spam

Spam is usually unsolicited junk e-mail sent to large numbers of people to promote products or services. The main effect is usually just annoying, but it can also cause performance problems to an organization that could be used as a mail relay for this spam.

Spam e-mail can also be malicious. Malicious spam can use software security holes as well as human actions to fulfil its role. A good example is phishing: the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private or sensitive information, which will be used for identity theft. Phishing is a form of social engineering.

3.3.4 Spying

Spying techniques can be used on a network (eavesdropping) or on a system (spyware). They usually consist of installing software on a system to gather information on the system or networks.

The growth of wireless networks (802.11, Bluetooth) has made network spying much easier because a physical access to the network is no longer necessary.

Although spying can take many forms and have many purposes, a common approach today is the use of spyware. Spyware is usually installed on a computer as part of a legitimate Internet access, and is then used, unbeknown to the user, to gather information on Internet browsing habits. Although many forms of spyware are harmless, there is no reason why this class of software cannot be used to collect passwords and credit card numbers. The results are usually sent back via the Internet to the interested parties.

One of the most dangerous forms of spying is a class of software called keyloggers. Once installed on a computer, these systems can collect every keystroke, mouse movement and screen update on a computer, thus allowing a hacker to obtain all privileged information before it is encrypted or after it is decoded. Keyloggers can also be of the hardware variety, often placed in line on USB ports, and can use their own wireless connectivity to report what they gather back to an off-site system.

3.3.5 Root or domain controller access

Hackers try to obtain access to the most privileged user or account in order to gain control of the entire network. Keeping passwords hard coded in the software or saved in flat files or in spreadsheets should be avoided.

3.3.6 Wireless Local Area Networks

Wi-Fi has become an accepted method of connection for mobile devices. Mobile devices connect to a Wi-Fi access point to access Internet Protocol (IP) services. These services can be replicated by “imposter” systems to look like official Wi-Fi services, but can act very differently. For example, when they are used to access the Internet, they can locally show a web page to be secure when accessed, but the secure access is only to the imposter device, not the end website. User information including passwords and keys can then be captured in the open, and used to steal personal information and access services.

Users are less likely to be vulnerable if they are accessing Internet services through a Virtual Private Network (VPN) tunnel to their home organization. The use of split tunnelling (where Internet services are accessed locally) increases the risk and is not recommended for corporate use.

It is possible for the Wi-Fi of official organizations to detect and suppress these imposter access points, but this is unlikely where the environment is not controlled. In a public space, there is a need to be vigilant for Wi-Fi services that have multiple similar names, or if in doubt, someone in charge should be asked which service to use.

4 IMPACTS OF THREATS AND SECURITY EVENTS

It is clear that multiple threats exist which have the capability to compromise or degrade both the assets of an organization’s IT systems as well as its capability to deliver information to the public and partner organizations.

Although it can be difficult to predict exactly what the impacts might be, the following are key potential impacts, which can be used to prepare security plans and contingency plans. Understanding the potential impacts is also important in justifying the funding for security measures, as the cost of repair, loss of business, loss of reputation and even loss of life often far exceed the cost of mitigation measures.

It should also be noted that although some events may seem to have a low impact at first, they could be of major importance to an organization at a later date, as many events are just part of a set-up process for later events. In addition, because organizations can be interconnected, these types of events can be set-ups for attacks in other organizations. In this respect, it is important to note the responsibility to the community of interconnected systems.

4.1 System and service impacts

This section lists the impacts that disrupt or incapacitate actual systems or services. These impacts affect the capability to deliver services to various degrees:

- *System slowdown:* Events cause the systems to slow down for no apparent reason. These performance problems can range from being a simple annoyance to being major trouble. Usually, the systems do not crash completely. The behaviour can be intermittent, which makes troubleshooting and problem resolution even more difficult. If not addressed, these events can last a long time, and eventually consume unnecessary system resources. The public, clients and partners will experience degraded service, which may lead to frustrations, loss of confidence and even loss of business. These types of problems can be the most complex to fix, as they are often not even noticed. Intrusion detection systems and regular system verifications are a great help in this regard.
- *System rendered unavailable:* Events cause the systems to stop functioning altogether. Several types of events may cause this. Usually, when the problem is removed, the systems will resume normal operation without other impacts. The problems cause obvious loss of service (affecting the users) and waste of valuable time of the system analysts and operation personnel that need to restart and clean infected components.
- *System or component of system or data destroyed:* Events cause not only the systems and services to not be available for a period of time, but cause the destruction of resources. Typically, this can be the destruction of data on storage media or stored in the database. Some viruses have been demonstrated to harm hardware by putting it in states that it was not designed to be in. These problems waste much time, but also require system components to be either replaced or reinitialized. There is often an important cost associated with these repairs.
- *System apparently normal, but information stolen or compromised:* Events that lead to these impacts usually reside on the systems in a way that is not detected. However, they may steal information that is copied back to remote systems or compromise information on the organization’s systems in various ways. The most obvious example of compromising information is called website defacement. However, more subtle changes are possible, which are difficult to detect. The impacts can be severe, as stolen information can be of sensitive or commercial nature. Compromised information may have public safety implications or political,

religious, sexual or racial contents. The organization's reputation and future may be at stake, as well as safety of life.

- *System used to compromise others:* Events would compromise an organization's systems in a way that is not detected, and may be left unused for a long time. However, these components can be used to compromise other systems. Although the impact on a given organization may seem negligible, harm to other organizations is possible. Furthermore, hackers often use such techniques to hide themselves behind several layers of obscurity as a disguise. These layers render troubleshooting very difficult and provide much hiding space for illicit components. An organization could be falsely accused of being the source of trouble because of this technique.

4.2 Administrative, legal and reputation impacts

In addition to the obvious system and service impacts, all security events can also cause administrative, legal and reputation impacts. By being connected to the Internet, all organizations need to act as good corporate citizens. They must mitigate the problems of security and ensure they are not the cause of problems to others. Failure to do so may eventually lead to legal action. It is also obvious that bad information and poor service will certainly have administrative impacts, as well as the loss of reputation. This is particularly important in the weather business, where State agencies have an important responsibility for the health and safety of their citizens.

The perception that a member in the Global Telecommunication System (GTS) community may be compromised can lead to a series of restrictions or concerns that this may be a threat to connected agencies. Members may isolate one another until further information on the issue is sought. This can take some time as it may involve national intelligence counterparts. During this period, the exchange of critical meteorological information across the world may be disrupted, reducing the quality of services offered.

5 INFORMATION TECHNOLOGY SECURITY PROCESS

The ISO 27000 family of standards helps organizations to keep their information assets secure. ISO/IEC 27001 is the best-known standard in the family, providing requirements for an information security management system.

The steps in the ITS process are described below.

5.1 Identify assets

The first step is to identify an organization’s assets. Formal methods recommend starting from the organization’s missions to specify which assets are necessary to fulfil these missions.

Security criteria that are important for the organization must then be defined, so that each asset’s security needs can be expressed regarding these criteria. The most common ones are availability, integrity and confidentiality.

5.2 Threats and risk assessment

Threats regarding vulnerabilities and methods of attack can then be analysed.

Risk assessment is carried out by evaluating threats with their impact on critical assets.

5.3 Business continuity planning

Business continuity planning, often referred to as disaster recovery, is the process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with minimal interruptions of service.

5.4 Prevent

Once an organization has properly identified its ITS requirements, prevention measures must then be set up to prevent or restrict an error, omission or unauthorized intrusion.

5.5 Detect

Monitoring and reporting should give the organization proper visibility on its information system. They must be defined so that a security incident can be quickly detected and its origin properly identified.

5.6 Respond and recover

Incident handling and disaster recovery procedures are essential to minimize the impact of an ITS-linked incident within an organization, by reacting quickly and in a proper manner to the incident, and by being able to recover the essential elements affected by the incident.

5.7 Investigate and correct

Once the incident is over, it must be analysed so that prevention measures and incident handling and disaster recovery procedures can be reviewed, if necessary.

6 BEST PRACTICES IN INFORMATION TECHNOLOGY SECURITY

6.1 Information Technology system security

IT system security in this context includes application, operating system, data and network security. The following paragraphs refer to network and operating system security only. Application and data security will be addressed in an update to this publication.

Section 2.3 defined security criteria. Different techniques have to be considered to fulfil these criteria in the context of network and system security.

Availability

> Availability is assured through network and system protection, physical redundancy, well-trained personnel and service contracts. Nevertheless, an availability of 100% can never be guaranteed. Service level agreements have to be in place that define minimum criteria for the different components. To ensure these service contracts, appropriate quality assurance must be in place.
> Network and system protection is a key factor in guaranteeing a certain level of availability by averting malicious activity through worms, viruses, Trojans, hackers, etc.

Integrity

> System integrity is assured through network and system protection, host-based or network-based intrusion detection/prevention systems and an appropriate backup/restore strategy.
> Data integrity can be assured through cryptographic measures such as hash and signing algorithms.

Confidentiality

> Confidentiality is achieved through organization, system and cryptographic protection measures.

Accountability

> Accountability is achieved through logging of system access and authorization wherever possible.

A key measure for all security criteria is network and system protection. A key technology for network protection is using firewall systems. The most common use for firewall systems is a central firewall between the internal network and the Internet, based on a proper zoned design. However, depending on the complexity of the internal network, distributed firewall systems should be put in place to protect sensitive internal network zones and systems, for example, databases and servers running critical services, from more dangerous parts, for example, network zones connecting user personal computers (PCs) and workstations (see section 6.2). Network protection can also be improved by introducing an intrusion detection/prevention system (IDS/IPS) to monitor the network traffic at certain points and to detect unwanted or suspicious traffic according to the security policy (see section 6.5).

System protection is more complex. The following measures have to be taken:

- *Access control:* Make sure that only authorized personnel have both physical and electronic access to a system. In addition, authentication has to be of appropriate strength (for example, appropriate password policy and certificate- or token-based authentication). In addition, logging is important to trace user activity, especially on mission-critical systems. Hence, group-based accounts (where a single account is used and the password shared between users) must be avoided wherever possible.
- *Minimize services:* Disable all services and processes that are not necessary for system operation and service offerings.
- *Backup strategy:* Make regular backups and archive these, so that a broken or compromised system can quickly be restored when necessary.
- *System integrity:* Use host-based intrusion detection systems to help assure system integrity by monitoring file system activity and by protecting mission-critical files and services.
- *Diversification and redundancy:* Make mission-critical services, such as Domain Name System (DNS) servers, customer-related web and File Transfer Protocol (ftp) servers, database servers and e-mail relays, redundant. Make sure that these redundant servers and gateways are physically separated to protect the overall system from fire, flooding, etc.

6.2 Network architecture

Network architecture plays a major role in overall network and system security. Several aspects have to be taken into consideration when designing networks in order to make them as secure as possible in the context of the discussion in section 6.1.

Two types of networks have to be distinguished. Local Area Networks (LANs) interconnect hosts and servers. They are used to pool end systems such as PCs, and to set up service networks by hosting a single server or a server farm offering certain services or applications, such as web services or database services, to personnel and customers.

Wide Area Networks (WANs) are used to interconnect networks that can be LANs or other WANs. A WAN normally does not offer host- or server-based services; however, it might have protected connection points when interconnecting networks with different security demands. These connection points can be routers with access lists or even complex firewall systems. Both are used to allow specific services only.

Virtual networks can be set up on top of physical networks or other virtual networks. There are numerous types of virtual networks. The most popular are:

- *VLANs:* Virtual LANs are used to segment a LAN-based intranet into different network zones; a VLAN is built on top of a LAN and is based upon Ethernet packet tagging according to the Institute of Electrical and Electronics Engineers (IEEE) standard 802.1q.
- *VPLS:* Virtual Private LAN Service is a way of providing Ethernet-based multipoint to multipoint communication over IP or Multiprotocol Label Switching (MPLS) networks.
- *Internet Protocol Security (IPSec) VPNs:* VPNs are typically IP based and use IPSec for data signing, and/or encryption according to the Request for Comments (RFC) 2401 (RFCs are available at www.ietf.org/rfc.html); VPNs are built on top of WANs and LANs.
- *MPLS:* This is a switching technology, and good descriptions are available in RFC 2547, RFC 2917, RFC 3031 and RFC 3034 for Frame Relay WANs.

Care should be taken with encrypted virtual networks such as IPSec-based VPNs that are set up in tunnel mode versus VPNs in transport mode, which make use of data signing only. As data are encrypted, virus scanners, intrusion detection/prevention systems and other centralized security measures may not work. Additional measures have to be taken at the VPN end points where the unencrypted data are available. Alternatively, crypto-gateways that decrypt the incoming and/or outgoing datastreams to check for viruses and other malicious contents can be established at sensitive network interconnections. After all checks have been completed, the data are re-encrypted with the gateway's own keys. However, legal issues have to be taken into account, especially if private usage, for example home banking, is not forbidden.

6.2.1 Local Area Networks

A LAN is usually a very heterogeneous aggregation of PCs, hosts and servers with a variety of offered services, communication relations and security demands.

Network segmentation increases overall network and system security in the context of the discussion in section 6.1 by grouping systems into appropriate groups that have similar communication profiles and security requirements.

A communication profile could be defined by the offered service (for example, Simple Mail Transfer Protocol (smtp), ftp or Hypertext Transfer Protocol (http)) and the communication direction or network location (for example, internal workstations or servers, outbound public servers or bidirectional gateways). Systems with similar profiles and similar security requirements may share one LAN segment (network zone), while systems with different profiles or different security requirements may be connected to disjunctive segments.

The reason for separation is that each service might have security vulnerabilities that could cause intruders (worms, viruses, Trojans, bots, hackers, etc.) to take over a system. Heterogeneous segments simplify hostile scans and attacks because of the larger number of different services within one segment. For example, web servers and ftp servers both serving requests from Internet users should not share a LAN segment because of their different traffic profiles. In addition, PCs should not be co-located with database servers because of the database servers' high security requirements for availability, integrity and potential confidentiality, while PCs are always at risk of Internet worms, Trojans and other malicious software.

The host (or PC) in the internal network must strictly follow the security policy of the corresponding network zone, and invalid external connection detection software should be installed in the host, which could access the critical IT resource. The LAN segments that connect the most critical IT resource or the sensitive data should be physically isolated, which can be requested by national legislation.

To protect the disjunctive network segments from each other, they should be interconnected through appropriate separation systems.

An aggregation of private LANs and LAN segments is referred to as a private intranet.

The security of an Ethernet LAN or LAN segment can be increased by using ISO/OSI (Open Systems Interconnection) layer 2 switching technology instead of broadcast media, so that traffic from a host A to another host B cannot be sniffed by a third-party host C. However, layer 2 switching cannot avert the so-called Address Resolution Protocol spoofing. Additional security measures, such as Port Based Network Access Control in conjunction with the use of host certificates, either based on registered hardware addresses or as defined in IEEE standard 802.1x, have to be taken into consideration to protect LANs from such attacks. Port-based access control makes sure that hosts which have not been registered cannot be connected to the network.

6.2.2 Wireless Local Area Networks

Securing Wireless LANs (WLANs) is critical with regard to availability, integrity and confidentiality:

- *Availability:* WLANs are highly sensitive to electromagnetic disturbances. A jammer could cause one or more WLAN cells to break down, so that legal WLAN devices cannot connect to the network any more.
- *Integrity and confidentiality:* Cryptographic measures have to be taken to guarantee data integrity and data confidentiality, if required. In particular, authentication data such as user names, passwords and token codes have to be encrypted to avert scanning and spoofing. One such method could be to use IEEE standard 802.1x.

The following measures have to be taken to protect WLANs and other network zones that are connected to WLANs:

- *WLAN footprint:* Make the reception area of a WLAN (footprint) match only the area of intended coverage. Make sure that WLAN radio cannot be received outside desired borders. Use a WLAN radio scanner for verification.
- *Radio shielding:* Make sure mission-critical WLANs are protected from radio jammers by shielding the walls and windows of those rooms where WLAN transceivers are operated. Furthermore, shielding protects the WLANs from being scanned, which is recommended, even though encryption is in use.
- *Encryption:* Use encryption on WLANs. Choose the best available encryption algorithm and change the default settings before activating WLANs. For user authentication and data encryption, use on-top encryption such as IPSec or Transport Layer Security, with at least 128 bit symmetric key lengths.
- *Network zoning:* Never attach a WLAN to another, more secure, network zone without a firewall in between. Even if the WLAN itself is well protected, a firewall has to be in place to limit access to just the services required. Use the firewall or an additional gateway for user authentication to force even authenticated WLAN users to authenticate themselves another time with a different password, certificate or token before accessing a more secure network zone. Make sure that appropriate authorization rules are in place to limit access to other, more secure network zones, even for authenticated users.
- *Monitoring and logging:* Monitor and log all WLAN activity, especially who is logged on and what they are doing. Analyse the log files at regular intervals.
- *Intrusion detection:* If necessary, install an IDS/IPS for additional security. Note that an IDS/IPS does not work well for encrypted network zones. However, the IDS/IPS can monitor communication relations and can generate alarms in case of illegal activity up to ISO/OSI layer 4, for example, port scans.
- *Protecting access:* Use a mechanism to protect the wireless network from unauthorized access, for example, 802.1x or WPA2 (Wi-Fi Protected Access version 2).

6.2.3 Firewall systems

Firewalls can be divided into two major groups:

- Packet filters;
- Application Layer and rule-based (also known as next-generation firewalls) Gateways.

Packet filters control network traffic up to ISO/OSI layer 4 (transport layer). A packet filter can be stateless or stateful. A stateless packet filter firewall separately analyses incoming packets independently of the Transmission Control Protocol (TCP) connection or User Datagram Protocol (UDP) datastream that they belong to.

A stateful firewall is connection aware and assigns each received packet to the related TCP connection or UDP datastream. In contrast to stateless firewalls, a stateful firewall drops all packets that do not belong to a previously established TCP connection or UDP datastream.

Application Layer Gateways have to be stateful in order to assign incoming packets to their respective connections and to reassemble the datastream in order to analyse the higher level protocols (ISO/OSI layers 5–7).

Application Layer Gateways work up to ISO/OSI layer 7 (application layer). To handle different high-level protocols such as ftp, http, smtp, etc., these firewalls require appropriate internal or external protocol engines. Most Application Layer Gateways can interpret and analyse standard protocols such as http, smtp and ftp off the shelf.

Non-standard, especially proprietary, protocols require external, customized gateways. For performance reasons, it might also be necessary to set up external gateways, even for protocols where the firewall is equipped with protocol engines. External gateways can easily be clustered to increase overall performance. Clustering utilizing external gateways is mostly cheaper than clustering the firewall appliances.

A complex firewall system might comprise different servers and gateways:

- DNS servers;
- Web servers;
- Ftp servers;
- E-mail relays;
- Web proxies;
- VPN gateways;
- Telephone dial-in servers.

These gateways and servers have different communication profiles and different security requirements, as described above.

Old firewall systems consisted of an external and an internal packet filter or an external packet filter and an internal stateful firewall with a so-called demilitarized zone (DMZ) in between. The servers and gateways that had to communicate with the Internet were placed into the DMZ. The disadvantage of this architecture was that the DMZ servers and gateways cannot be separated to meet their individual communication profiles and security requirements.

Modern firewall appliances have both an internal and an external packet filter, or a packet filter and a stateful firewall with protocol analysers in one single box. The former DMZ has become the so-called service network (SN). Instead of one SN, today's firewall appliances offer multiple SNs, so that firewall servers, gateways and proxies can be separated according to their individual communication profiles and security requirements. This allows for a firewall zone concept that increases overall network security by protecting mission-critical servers and gateways through optimized firewall rules.

Formerly, only one firewall system has been used to protect the intranet from the Internet. Today, intranets are partitioned into different network zones. These network zones are protected by firewalls or firewall systems to meet their individual security demands (distributed firewall architecture). Less-secure network zones hosting PCs and user workstations might be protected by simple packet filters, while zones hosting central database servers may require more complex application layer firewall systems with SQL (Structured Query Language) gateways and intrusion detection systems.

Note that the GTS network also has to be protected from private intranets and vice versa. A firewall system should be in place to limit access to the services required.

While a firewall always reassembles incoming IP packets to prevent attacks caused by fragmentation, access lists on routers do not reassemble fragmented packets. Therefore, access lists cannot always be considered as a substitute for a firewall.

6.3 Remote access

Remote access to network resources is one of the most critical applications with regards to network security. Remote-access systems can be:

- Plain Old Telephone Systems, Public Switched Telephone Networks or Integrated Service Data Networks dial-in servers;
- Secured Internet access (VPN gateways based on IPSec or Secure Socket Layer).

There are four items that have to be taken into consideration when designing and operating remote access:

- *Network architecture:* Remote-access servers have to be placed into a separate network zone to protect other zones from possible malicious traffic. Best practise is to set up a dedicated firewall zone, or a distinct SN for remote-access servers only. This allows for maximum control over traffic passing through. If there are different remote-access servers for internal personnel and external staff, such as support personnel, the corresponding access servers should also be placed into separate networks or firewall zones.
  The GTS network, for example, should never be connected to the same network zone as remote-access systems.
  If it becomes necessary, for example for maintenance and monitoring, to access the GTS or any other mission-critical network zone from remote-access servers, appropriate access or firewall rules have to be in place in order to limit the access to just the services required. Network zones with remote-access servers must never be directly connected to other network zones. There must always be appropriate packet filters or firewalls in between.
- *User authentication:* In particular, for remote-access systems, proper user authentication is essential for overall network security. Strong authentication mechanisms such as certificate- or token-based or multifactor methods are preferred over weak, password-based methods.
- *User authorization:* Even authenticated users must not be able to obtain access to all systems. Authorization rules have to be in place to limit access to systems that the user is authorized for. For easy maintenance, authorization should be based on groups rather than on per-user rights. A user may be a member of several groups, granting the individual all the rights of each group. The host that is being used by an authorized user to get access to an internal system should meet the security requirements.
- *Logging and accounting:* For surveillance and troubleshooting reasons, an appropriate logging and accounting mechanism has to be in place. In case of malicious activity or other illegal activity, log files are necessary to trace back system failures or intruders. Furthermore, accounting may be required for billing.

6.4 Server access and security

In addition to remote-access servers, there are a number of other systems that require access control such as data distribution servers, ftp servers, web servers or database servers.

Two access methods have to be distinguished:

- Anonymous access;
- Pre-authorized access.

Anonymous access is widely used for the Internet, especially for public web and ftp servers. Data distributed by anonymous servers are not confidential. However, data integrity is still an issue in order to prevent data manipulation by hackers, worms, viruses, etc. In addition to the measures described in section 6.1, it has to be ensured that:

- The anonymous service (for example, ftp, http or smtp) is minimized. The command interface must be as minimal as possible. Unnecessary commands must be deactivated. A user of such a system should get just the commands required to access data.
- Non-public data are not accessible. Either all non-public data must be removed from the server and stored elsewhere or it must not be possible to access these data through the public interface. Potential security holes must be assessed. Also, the operating system and configuration files of the service must be protected from external access.
- The servers are well patched against all known security holes. The latest patches must have been applied. Patches must be verified in accordance with change and configuration management processes prior to being installed on mission critical systems.

In addition to authorization mechanisms, appropriate logging and accounting has to be in place in order to be able to monitor user and system activity, as well as to trace back malicious activity. Accounting and billing mostly does not apply to anonymous access systems.

In contrast to anonymous data distribution servers, pre-authorized systems may have to be secure regarding data confidentiality. Measures have to be taken to protect these systems from unauthorized access. An appropriate authentication mechanism has to be in place to assure that only authorized users gain access to such systems. Depending on the security requirements of the systems and the stored data, adequate authentication methods have to be in place (see the table below).

Potential authentication methods

Security requirement	*Authentication method*
Low	Password protection
Medium	Token/certificate-based protection
High	Twofold protection, for example, a token or certificate protected by a Personal Identification Number

Minimizing user interfaces, establishing authorization rules and logging also applies for pre-authorized access systems, and accounting and billing might become necessary for systems with well-known users.

Systems that serve anonymous users should be separated from pre-authorized systems that store confidential data. They should be located in separate firewall zones. Never operate both anonymous and pre-authorized services on one single machine.

Anonymous access systems should be avoided whenever possible. They should only be used for data distribution to the public domain.

For private data exchange, for example, between countries across the GTS or the Internet, only pre-authorized systems may be used.

6.4.1 File system authorization rules

Both anonymous and pre-authorized systems require strict authorization rules. By default, only read access should be allowed. Write access should only be allowed when required. Systems with write access should have dedicated directories to store the data and to scan for viruses and malicious code before making them available to internal resources or users.

Sometimes, it might be required to only accept signed data to verify data integrity. Unsigned data or data with wrong hash values will then be rejected. Data signing is an effective way to guarantee data integrity and authenticity. However, public key infrastructures or PGP (Pretty Good Privacy) infrastructures have to be in place to provide and manage the required certificates.

6.5 Security policies

6.5.1 Requirement for a security policy

In order to properly design and implement any security mechanism, it is essential to define a security policy. The policy documents what is expected of users, what can be expected of the system, and how all of this will be carried out between the many groups that all have a responsibility in security. It is a guideline that explains what the organization admits as acceptable and unacceptable configurations. In doing so, it sets a level that is a key statement for the implementation of security. The level is set by identifying the risks and determining what is required to mitigate them at an acceptable level for the organization.

Depending on the complexity of the organization, there may actually be several types of security policy documents.

At the highest level, there would be a program policy describing the overall organization’s security approach. It usually describes who is responsible for the different aspects of security (physical, electronic, people, etc.). It may also provide direction for compliance with industry standards such as those of ISO.

At other levels, there could be issue-specific policies, such as password policies, electronic network usage policies, web-server policies or remote-access policies.

6.5.2 Developing a policy

It would be nearly impossible to develop a WMO-wide security policy as different governments and agencies have various and potentially incompatible policies around the world. However, every Member should develop its own policy, taking into account the factors described in this publication.

In order to develop the security policies, a team should be formed with representatives of the IT department, but it should also include human resources, physical facility management and senior management.

The general high-level security policy of an organization can be designed using some of the industry standard examples that are readily available on the Web. Two of these are well recognized and available free of charge:

– SysAdmin, Network and Security (SANS) (http://www.sans.org/security-resources/policies/);

- Cisco Network Security Policy White Paper (http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014f945.shtml).

For issue-specific policies, an organization can construct policies based on existing implementation and maintenance procedures. The policy should provide answers to the following questions:

- Who does the procedure?
- What is the procedure for?
- Why is the procedure done?
- When is the procedure done?
- Where is the procedure done?

It will often be found that these questions do not have clear answers in an existing organization, just because there is no stated policy. This exercise can be quite enlightening.

The policies should be easy to read, precise and realistic. Good policies will also be consistent with each other and forward looking, considering that there are always new risks and new technology.

In addition, policies should be regularly reviewed to ensure they continually reflect the security needs of the organization, and to take into account any changes in security practise within the wider IT community.

Finally, policies should be approved and signed by an appropriate authority in the organization. Again, as security is the matter of several (if not all) components of an organization, only such an authority will ensure consistency in approach and in implementation.

6.6 Threat and risk assessment

Threat and risk assessment (TRA) is a process in which an evaluation of the potential security problems that might affect an organization is carried out. It usually consists of an identification of threats and vulnerabilities to derive an evaluation of the relative risk. The risk can also be described in terms of likelihood, impact and consequence. This is particularly useful in estimating a cost for particular risks. These cost figures help in the design of the proper level of security measures. For example, a low-risk/high-consequence threat may justify an expensive security measure.

TRA can be carried out with a very general scope to kick-start the process of determining a security policy and security procedures. It can also be done on a regular basis with a much more refined scope, to ensure that the security measures in place are still adequate. In both cases, the goal of the TRA is to identify the exposure or the potential for loss or harm and to serve as a basis for improvement of the security measures.

Depending on the organization, TRA can be quite complex to accomplish. In addition, it is often a good idea to obtain an unbiased opinion from an outside party, as it should be noted that threats can be internal or external, and can also be intentional or accidental. It is therefore usually recommended that TRA be conducted by outside specialists. Most large reputable IT consulting firms are well equipped to carry out this kind of work.

6.7 Policy control

Once the security policy and procedures have been implemented, it is necessary to perform regular controls to ensure that the rules are adhered to and that new threats can be identified. These controls usually consist of a combination of procedures, metrics and audits.

The procedures and metrics are usually automatic mechanisms that suggest or force certain security behaviours, for example, automatic reminders to change passwords, counts of rejected user identification attempts or automatic monitoring of web browsing and volume of traffic. These mechanisms can run continuously and provide information to security managers on a day-to-day basis about the status of the systems.

The audits are more in-depth analyses of the security situation and are meant to improve areas that are not readily visible or measured by the other mechanisms. The audits should be based on the security policies and proceed to verify that they are adhered to.

6.8 Procedures

The following subsections outline the basic procedures that are essential for ensuring that systems are kept secure.

6.8.1 System management

Organizations must have system administrators who keep a clear view of all system components and manage all the servers, desktops and network equipment on an ongoing basis.

6.8.2 New system installation and change management

All new systems or new system components should be introduced in the production environment through a predefined installation procedure. This procedure should include at least the following steps:

- Suppress all the accounts that do not have passwords;
- Back up all configuration files;
- Ensure software is up to date according to the organization configuration and version control processes, and keep a list of components and version numbers;
- Suppress network services that are not necessary;
- Configure and install a logging system for all important system activities.

All changes should be tracked to control the system components and be capable of tracing unwanted changes.

6.8.3 Installation of security patches

Follow the security advisories from the Computer Emergency Response Team (CERT) (for example, http://www.us-cert.gov, https://www.dfn-cert.de/en.html, https://www.cert.be or http://www.cert.ssi.gouv.fr/) and install patches as soon as they are available.

6.8.4 User account management

- All accounts must belong to a specific user;
- Each user should read and understand the organization’s security policy;
- End-user accounts that are unused for a period of time (3 months) should be deactivated;

- A password policy that outlines the requirements for password complexity, strength and duration should be defined, and this policy should be known by all users;
- Remote-access users should use one-time password systems to eliminate the possibility of password capture by illicit users.

6.8.5 Backup/restore procedures and regular testing

System administrators should develop and maintain adequate backup and restore procedures to be capable of recovering lost data in case of disaster. The restore procedures should be tested regularly.

6.8.6 Detection procedures

Several detection procedures can be put in place to monitor system activity and possible illicit or unwanted activity. These procedures should be 24/7 and can include intrusion detection and prevention, abnormal system activity detection, vulnerability scanning, loss of system or loss of data procedures.

6.8.6.1 *Protection from malicious codes*

Real-time antivirus systems should be installed and applied where appropriate. Whole-of-server scans should be run on a daily basis. Antivirus software should be configured in real-time mode to ensure any infections are identified and cleaned immediately upon detection.

A separate server or computer should be configured to sit inside the organization’s firewall in real-time mode. This server should be configured with appropriate software to check for malicious code. If such a code is detected and all incoming and outgoing e-mail attachments can be cleaned, then the message can be distributed. If attachments cannot be cleaned, then the message should be blocked.

Typical controls to protect against malicious use technology, policies, procedures and training, applied in a layered manner from the perimeters inward to hosts and data. They should be applied at the host, network and user levels.

6.8.6.2 *User education*

Users should be educated about malicious software in general, the risks that it poses, virus symptoms and warning signs, including what processes should be followed in the case of a suspected virus. Organizations should consider network broadcasts or a system for alerting users of virus attacks.

6.8.6.3 *Unauthorized software*

Agencies should establish a policy outlining the prohibited use and installation of software not authorized by the agency including user responsibilities with regards to downloading software from Internet and e-mail sources.

6.8.7 Response/recovery procedures

In the case of a security event, a security threat and response procedure should be developed in order to identify key resources, personnel and actions to take in the case of problems. These procedures should be available 24/7, and can include steps for damage control (quick isolation of problem to limit its propagation), communication to concerned parties and partners, recovery of affected systems, maintaining essential services for mission-critical components and even shutdown procedures in case of severe events.

6.8.8 Security information and event management

It is recommended to implement a solution capable of monitoring, evaluating and correlating events related to security issues. This type of solution, known as Security Information and Event Management (SIEM), is a software-based solution that combines events and alerts provided by network agents in real-time mode. It behaves as a "landmine" in front of a system and helps to visualize or pay attention to what is going on, allowing actions to be taken in advance.

A SIEM solution allows events generated by various security applications (such as firewalls, proxies, intrusion prevention systems and antivirus software) to be collected, normalized, stored and correlated in order to enable rapid identification and response to incidents. A standard SIEM tool would include the following topics:

- Combination of the features offered in the technologies of Security Information Management and Security Event Management, with real-time access, and centralized and consistent to all logs and security events, regardless of the technology and manufacturer;

- Correlation of heterogeneous technologies logs, connecting common or significant attributes among sources, in order to transform the data into useful information;

- Identification of behaviour, incidents, fraud, anomalies and baseline breaks;

- Automated triggering of alerts and notifications in the event of non-compliance with security policies or regulatory standards, or according to pre-established business rules;

- Sophisticated reporting on environmental safety conditions for Security Operations Centre team auditing and incident response;

- Retention and indexing of long-term data, allowing subsequent forensic analysis;

- Auditing of event-log-related information.

6.9 Public server configuration

Public Internet accessible servers (web, mail or ftp) are increasingly being used by organizations to publish and exchange information. They play an important role in the public image for a growing number of people. Their exposure to the Internet raises the risk to a high level and deserves a brief discussion.

It is very important to minimize risks by securing such servers. Here are a few good practices:
(a) Architecture: Install the server in a dedicated zone, for example, a semi-private network that is visible through the network's firewalls, but that is not part of the private networks of an organization;
(b) Filtering:

(i) Protect the server from network access by a firewall filtering all network flows but the port used by the service to access the server;

(ii) If possible, the firewall should be able to analyse the protocol used (http relay) and to filter specific instructions, so that cracking attempts can be filtered before reaching the server;

(iii) The firewall should prevent IP spoofing;

(iv) The firewall should also be able to filter some network denial-of-service attempts (land attack, SYN flooding, etc.);

(c) Bandwidth: A bandwidth management tool should be used to avoid excessive use of bandwidth by a single user (or group of users);

(d) System/application:

(i) The server should process as few types of data as possible (for example, do not combine multiple server applications on the same virtual or physical system);

(ii) The server should be stripped of all unnecessary services and applications (see also section 6.1 on system security);

(iii) Host-based firewalls should be used;

(iv) Security-related operating systems and application patches and updates should be tested and applied as soon as possible;

(e) Users and administrators:

(i) The server should have as few users as needed;

(ii) Remote administration should be restricted;

(iii) The strongest authentication method should be used;

(iv) System administrators should be highly skilled in the appropriate technologies;

(f) Controls:

(i) Intrusion detection and other logs should be monitored frequently;

(ii) Vulnerability assessment tools should be run against the server frequently.

7 USEFUL RESOURCES FOR INFORMATION TECHNOLOGY SECURITY

The following resources can be useful for learning more about the ITS processes, finding up-to-date information on industry standard security procedures and establishing security policies:

- SANS (http://www.sans.org);
- CERT (http://www.cert.org/);
- Government ITS agencies;
- Center for Internet Security (http://www.cisecurity.org/);
- Internet Engineering Task Force security working groups (http://www.ietf.org/html.charters/wg-dir.html#Security%20Area);
- Request for Comments 2196 *Site Security Handbook* (https://www.rfc-editor.org/info/rfc2196);
- Information Security Policies and Standards Group (http://www.information-security-policies-and-standards.com/);
- National Institute of Standards and Technology (NIST) *Information Security Handbook* (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf);
- National Security Agency documents on securing systems (http://www.nsa.gov/);
- Internet Security Alliance guidance (http://www.isalliance.org);
- ISO guidance on ITS, such as the ISO/IEC 27000 series (http://www.iso.org/iso/home/standards/management-standards/iso27001.htm);
- http://en.wikipedia.org/wiki/Standard_of_Good_Practice;
- http://en.wikipedia.org/wiki/Cloud_computing_security;
- https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf;
- http://en.wikipedia.org/wiki/Information_security.

BIBLIOGRAPHY

Carr, J., 2011: *Inside Cyber Warfare*. Second edition. O'Reilly Media.

Cheswick, W.R., S.M. Bellovin and A.D. Rubin, 2003: *Firewalls and Internet Security*. Addison-Wesley.

Donahue, G.A., 2011: *Network Warrior*. Second edition. O'Reilly Media.

Kurtz, G., S. McClure and J. Scambray, 2009: *Hacking Exposed*. Osborne/McGraw-Hill.

Russell, R., Rain Forest Puppy and Muidge, 2002: *Hack Proofing your Network*. Syngress Publishing Inc.