INTERNATIONAL STANDARD

ISO/IEC 27032

Second edition
2023-06

Cybersecurity — Guidelines for Internet security

Cybersécurité — Lignes directrices relatives à la sécurité sur l'internet

Reference number
ISO/IEC 27032:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27032:2012) which has been technically revised.

The main changes are as follows:

— the title has been modified;

— the structure of the document has been changed;

— the risk assessment and treatment approach has been changed, with the addition of content on threats, vulnerabilities and attack vectors to identify and manage the Internet security risks;

— a mapping between the controls for Internet security cited in 9.2 and the controls contained in ISO/IEC 27002 has been added to Annex A.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The focus of this document is to address Internet security issues and provide guidance for addressing common Internet security threats, such as:

— social engineering attacks;

— zero-day attacks;

— privacy attacks;

— hacking; and

— the proliferation of malicious software (malware), spyware and other potentially unwanted software.

The guidance within this document provides technical and non-technical controls for addressing the Internet security risks, including controls for:

— preparing for attacks;

— preventing attacks;

— detecting and monitoring attacks; and

— responding to attacks.

The guidance focuses on providing industry best practices, broad consumer and employee education to assist interested parties in playing an active role to address the Internet security challenges. The document also focuses on preservation of confidentiality, integrity and availability of information over the Internet and other properties, such as authenticity, accountability, non-repudiation and reliability that can also be involved.

This includes Internet security guidance for:

— roles;

— policies;

— methods;

— processes; and

— applicable technical controls.

Given the scope of this document, the controls provided are necessarily at a high-level. Detailed technical specification standards and guidelines applicable to each area are referenced within the document for further guidance. See Annex A for the correspondence between the controls cited in this document and those in ISO/IEC 27002.

This document does not specifically address controls that organizations can require for systems supporting critical infrastructure or national security. However, most of the controls mentioned in this document can be applied to such systems.

This document uses existing concepts from ISO/IEC 27002, the ISO/IEC 27033 series, ISO/IEC TS 27100 and ISO/IEC 27701, to illustrate:

— the relationship between Internet security, web security, network security and cybersecurity;

— detailed guidance on Internet security controls cited in 9.2, addressing cyber-security readiness for Internet-facing systems.

As mentioned in ISO/IEC TS 27100, the Internet is a global network, used by organizations for all communications, both digital and voice. Given that some users target attacks towards these networks, it is critical to address the relevant security risks.

Cybersecurity — Guidelines for Internet security

1 Scope

This document provides:

— an explanation of the relationship between Internet security, web security, network security and cybersecurity;

— an overview of Internet security;

— identification of interested parties and a description of their roles in Internet security;

— high-level guidance for addressing common Internet security issues.

This document is intended for organizations that use the Internet.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
attack vector
path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome

EXAMPLE 1 IoT devices.

EXAMPLE 2 Smart phones.

3.2
attacker
person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

[SOURCE: ISO/IEC 27033-1:2015, 3.3]

3.3
blended attack
attack that seeks to maximize the severity of damage and speed of contagion by combining multiple *attack vectors* (3.1)

3.4
bot
automated software program used to carry out specific tasks

Note 1 to entry: This word is often used to describe programs, usually run on a server, that automate tasks such as forwarding or sorting e-mail.

Note 2 to entry: A bot is also described as a program that operates as an agent for a user or another program or simulates a human activity. On the Internet, the most ubiquitous bots are the programs, also called spiders or crawlers, which access websites and gather their content for search engine indexes.

3.5
botnet
collection of remotely controlled malicious bots that run autonomously or automatically on compromised computers

EXAMPLE Distributed denial-of-service (DDoS) nodes, where the botnet controller can direct the user's computer to generate traffic to a third-party site as part of a coordinated DDoS attack.

3.6
cybersecurity
safeguarding of people, society, organizations and nations from cyber risks

Note 1 to entry: Safeguarding means to keep cyber risk at a tolerable level.

[SOURCE: ISO/IEC TS 27100:2020, 3.2]

3.7
dark net
network of secret websites within the Internet that can only be accessed with specific software

Note 1 to entry: The dark net is also known as the dark web.

3.8
deceptive software
software which performs activities on a user's computer without first notifying the user as to exactly what the software will do on the computer, or asking the user for consent to these actions

EXAMPLE 1 A program that hijacks user configurations.

EXAMPLE 2 A program that causes endless popup advertisements which cannot be easily stopped by the user.

EXAMPLE 3 Adware and spyware.

3.9
hacking
intentionally accessing a computer system without the authorization of the user or the owner

3.10
hacktivism
hacking (3.9) for a politically or socially motivated purpose

3.11
Internet
global system of inter-connected networks in the public domain

[SOURCE: ISO/IEC 27033-1:2015, 3.14, modified — "the" has been deleted from the term.]

3.12
Internet security
preservation of confidentiality, integrity and availability of information over the *Internet* (3.11)

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

Note 2 to entry: Please refer to definitions on confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability in ISO/IEC 27000:2018, Clause 3.

3.13
Internet service provider
ISP
organization that provides Internet services to a user and enables its customers access to the *Internet* (3.11)

Note 1 to entry: Also, sometimes referred to as an Internet access provider (IAP).

3.14
malicious content
applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them

3.15
malware
malicious software
software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system

EXAMPLE Viruses, worms and trojans.

3.16
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: In the context of this document, an individual is distinct from an organization.

Note 2 to entry: In general, a government is also an organization. In the context of this document, governments can be considered separately from other organizations for clarity.

[SOURCE: ISO 9000:2015, 3.2.1, modified — Note 1 to entry and Note 2 to entry have been replaced.]

3.17
phishing
fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication

Note 1 to entry: Phishing can be accomplished by using social engineering or technical deception.

3.18
potentially unwanted software
deceptive software (3.8), including *malicious* (3.15) and non-malicious software, that exhibit the characteristics of deceptive software

3.19
spam
unsolicited emails that can carry malicious content and/or scam messages

Note 1 to entry: While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam and junk fax transmissions.

[SOURCE: ISO/IEC 27033-1:2015, 3.37, modified — Note 1 to entry has been added.]

3.20
spyware
deceptive software (3.8), that collects private or confidential information from a computer user

Note 1 to entry: Information can include matters such as websites most frequently visited or more sensitive information such as passwords.

3.21
threat
potential cause of an unwanted incident, which can result in harm to a system, individual or *organization* (3.16)

3.22
trojan
malware (3.15) that appears to perform a desirable function for the user but that mislead the user of its true intent

3.23
vishing
voice phishing done to acquire private or confidential information by masquerading as a trustworthy entity

Note 1 to entry: Vishing can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.

3.24
waterhole technique
technique inciting people to access a website that specifically contains (lots of) malware

Note 1 to entry: Waterhole is also known as watering hole.

3.25
World Wide Web
Web
universe of network-accessible information and services

[SOURCE: ISO 19101-1:2014, 4.1.40]

4 Abbreviated terms

The following abbreviated terms are used in this document.

AI	artificial intelligence
API	application programming interface
APT	advanced persistent threat
BYOD	bring your own device
CERT	computer emergency response team
DDoS	distributed denial-of-service
DLP	data loss prevention
DMZ	demilitarized zone
DNS	domain name system

DoS	denial-of-service
EDR	endpoint detection and response
FTP	file transfer protocol
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol over secure socket layer
ICANN	internet corporation for assigned names and numbers
ICT	information and communications technology
IDS	intrusion detection system
IETF	Internet engineering task force
IMT	incident management team
IoT	internet of things
IP	Internet protocol
IPS	intrusion prevention system
ISP	Internet service provider
ISV	independent software vendor
IRT	incident response team
ISMS	information security management system
OWASP	open web application security project
PII	personally identifiable information
SDLC	software development life cycle
SIEM	security information and event management
SME	small and medium enterprises
URL	uniform resource locator
USB	universal serial bus
VPN	virtual private network
W3C	World Wide Web consortium
WWW	World Wide Web

5 Relationship between Internet security, web security, network security and cybersecurity

Figure 1 shows a high-level view of the relationship between Internet security, web security, network security and cybersecurity.

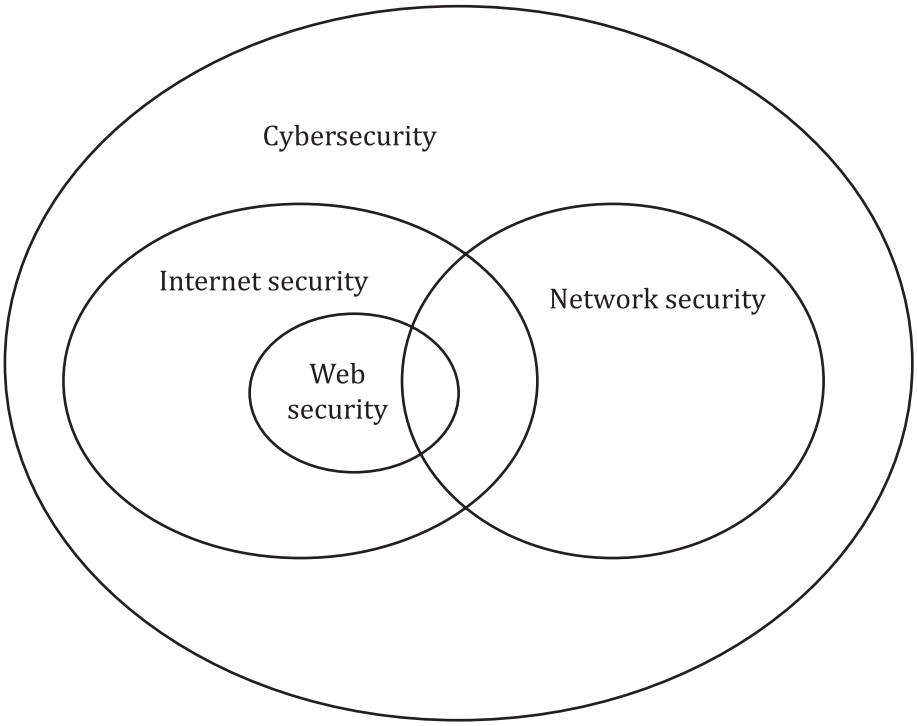

Figure 1 — Relationship between Internet security, web security, network security and cybersecurity

The Internet is a global system of inter-connected digital networks in the public domain. The information exchange on the Internet also uses the mobile telephony network that is hence part of the Internet. This global network connects billions of servers, computers, and other hardware devices. Each device is connected with any other device through its connection to the Internet. The Internet creates an environment which is conducive to information sharing.

Internet security is concerned with protecting Internet-related services and related ICT systems and networks as an extension of network security. These efforts aim to reduce Internet related security risks for organizations, customers and other relevant stakeholders.

Internet security also ensures the availability and reliability of Internet services. Over the Internet, various services are on offer, such as file transfer services, mail services or any services that can be publicly shared with the end users. In this context, Internet security deals with the secure delivery of these services over the public network.

The web is one of the ways information is shared on the Internet [others include email, file transfer protocol (FTP), and instant messaging services]. The web is composed of billions of connected digital documents that can be viewed using a web browser. A website is a set of related web pages that are prepared and maintained as a collection in support of a single purpose.

Web security deals with information security in the context of World Wide Web (WWW) and with web services accessed over the public network. The web service is enabled by the use of HTTP protocol in which any registered publicly available URL can be accessed. Web security also deals with security of this HTTP connection used for information exchange.

A network can include components such as routers, hubs, cabling, telecommunications controllers, key distribution centres, and technical control devices. Network security broadly covers all kinds of networks that exist within an organization from local area network, wide area network, personal area network and wireless networks.