国际的
标准

ISO/IEC 27032

第二版 2023-06

网络安全　　指南
网络安全

网络安全　Lignes 指导亲属进行互联网安全

参考编号
ISO/IEC 27032:2023(E)

受版权保护的文档

ISO 版权局 CP 401 ·
第 1 章de Blandonnet 8 CH-1214
Vernier, 日内瓦 电话：+41 22
749 01 11 电子邮件：
copyright@iso.org 网站：
www.iso.org

瑞士出版

内容

页

前言

ISO（国际标准化组织)和 IEC（国际电工委员会)构成了全球标准化的专业体系。作为 ISO 或 IEC 成员的国家机构通过各自组织设立的技术委员会参与国际标准的制定,以处理特定的技术活动领域。 ISO 和 IEC 技术委员会在共同感兴趣的领域开展合作。其他政府和非政府国际组织也与 ISO 和 IEC 合作参与了这项工作。

用于制定本文件的程序及其进一步维护的程序在 ISO/IEC 指令第 1 部分中进行了描述。特别是,应注意不同类型文件所需的不同批准标准。本文件是根据 ISO/IEC 指令第 2 部分的编辑规则起草的（参见www.iso.org/directives或www.iec.ch/members_experts/refdocs）。

ISO 和 IEC 提请注意本文件的实施可能涉及使用专利的可能性。 ISO 和 IEC 对任何所主张的专利权的证据、有效性或适用性不采取任何立场。截至本文件发布之日,ISO 和 IEC 尚未收到实施本文件可能需要的专利通知。但是,实施者请注意,这可能并不代表最新信息,最新信息可以从www.iso.org/patents和https://patents.iec.ch上提供的专利数据库中获取。 ISO 和 IEC 不负责识别任何或所有此类专利权。

本文档中使用的任何商品名称都是为了方便用户而提供的信息,并不构成认可。

有关标准自愿性的解释、与合格评定相关的 ISO 特定术语和表达方式的含义,以及有关 ISO 遵守世界贸易组织 (WTO) 贸易技术壁垒 (TBT) 原则的信息,请参见www .iso.org/iso/foreword.html。在 IEC 中,请参阅www.iec.ch/understanding-standards。

本文件由联合技术委员会 ISO/IEC JTC 1 （信息技术）、小组委员会 SC 27（信息安全、网络安全和隐私保护)编写。

第二版取消并取代了经过技术修订的第一版 (ISO/IEC 27032:2012)。

主要变化如下：

- 标题已修改；
- 文件的结构发生了变化；
- 改变了风险评估和处理方式,增加了威胁、漏洞和攻击向量的内容,以识别和管理互联网安全风险；
- 附录A中添加了9.2中引用的互联网安全控制措施与 ISO/IEC 27002 中包含的控制措施之间的映射。

有关本文件的任何反馈或问题应直接提交给用户的国家标准机构。这些机构的完整列表可以在www.iso.org/members.html和www.iec.ch/national-committees上找到。

介绍

本文档的重点是解决互联网安全问题,并为解决常见互联网安全威胁提供指导,例如:

社会工程攻击;

零日攻击;

隐私攻击;

黑客攻击;和

恶意软件、间谍软件和其他潜在有害软件的扩散
软件。

本文件中的指南提供了解决以下问题的技术和非技术控制措施:
互联网安全风险,包括以下方面的控制:

准备攻击;

防止攻击;

检测和监控攻击;和

响应攻击。

该指南的重点是提供行业最佳实践、广泛的消费者和员工教育,以协助感兴趣的各方在应对互联网安全挑战方面发挥积极作用。该文件还重点关注互联网上信息的机密性、完整性和可用性以及其他属性,例如真实性、责任性、不可否认性和可靠性

这也可能涉及。

这包括以下方面的互联网安全指南:

角色;

政策;

- 方法;

流程;和

适用的技术控制。

考虑到本文档的范围,所提供的控制措施必然是高层的。文件中引用了适用于每个领域的详细技术规范标准和指南,以提供进一步指导。请参阅附录 A了解本文件中引用的控制措施与 ISO/IEC 27002 中的控制措施之间的对应关系。

本文档并未具体讨论组织对支持关键基础设施或国家安全的系统可能要求的控制措施。然而,本文档中提到的大多数控件都可以应用于此类系统。

本文件使用 ISO/IEC 27002、ISO/IEC 27033 系列、ISO/IEC TS 27100 和 ISO/IEC 27701 中的现有概念来说明:

互联网安全、网络安全、网络安全和网络安全之间的关系;

9.2中引用的互联网安全控制的详细指南,解决了网络安全准备问题
面向互联网的系统。

正如 ISO/IEC TS 27100 中提到的,互联网是一个全球网络,组织使用它进行所有通信（包括数字和语音）。鉴于一些用户针对这些网络进行攻击,解决相关的安全风险至关重要。

网络安全　互联网安全指南

1 范围

本文件规定：

解释互联网安全、网络安全、网络安全和网络安全之间的关系
网络安全；

互联网安全概述；

利益相关方的识别及其在互联网安全中的作用的描述；

解决常见互联网安全问题的高级指南。

本文档适用于使用 Internet 的组织。

2 规范性引用文件

正文中引用下列文件时，其部分或全部内容构成本文件的要求。对于注明日期的参考文献，仅引用的版本适用。对于未注明日期的参考文献，适用参考文件的最新版本（包括任何修订）。

ISO/IEC 27000，信息技术　安全技术　信息安全管理系统　概述和词汇

3术语和定义

就本文件而言，ISO/IEC 27000 中给出的术语和定义以及以下内容适用。

ISO 和 IEC 在以下地址维护用于标准化的术语数据库：

ISO在线浏览平台：https: //www.iso.org/obp

IEC Electropedia：可在https://www. electropedia.org/获取

3.1
攻击向量
攻击者可以访问计算机或网络服务器以传递恶意结果的路径或手段

示例 1 物联网设备。

示例 2 智能手机。

3.2
攻击者
故意利用技术和非技术安全控制中的漏洞来窃取或破坏信息系统和网络，或破坏信息系统和网络资源的合法用户的可用性的人

[来源：ISO/IEC 27033-1:2015, 3.3]

3.3
混合攻击通过组合
多个攻击向量来寻求最大化损害严重程度和传染速度的攻击(3.1)

3.4
bot
用于执行特定任务的自动化软件程序

注 1:该词通常用于描述通常在服务器上运行的程序,这些程序可自动执行转发或排序电子邮件等任务。

注 2:机器人也被描述为作为用户或其他程序的代理运行或模拟人类活动的程序。在互联网上,最普遍的机器人是程序,也称为蜘蛛或爬虫,它们访问网站并收集其内容以用于搜索引擎索引。

3.5
僵尸网
络在受感染计算机上自主或自动运行的远程控制恶意机器人的集合

示例 分布式拒绝服务 (DDoS) 节点,其中僵尸网络控制器可以引导用户计算机生成流向第三方站点的流量,作为协调 DDoS 攻击的一部分。

3.6
网络安全保护人
民、社会、组织和国家免受网络风险

注 1:保障意味着将网络风险保持在可容忍的水平。

[资料来源:ISO/IEC TS 27100:2020, 3.2]

3.7
暗网 互联
网内只能通过特定软件访问的秘密网站网络

注1:暗网也称为暗网。

3.8
欺骗性软件在用户的计
算机上执行活动而未事先通知用户该软件将在计算机上执行的具体操作或询问用户对这些操作的同意的软件。

示例 1 劫持用户配置的程序。

示例 2 一个程序会导致用户无法轻易停止的无休止的弹出广告。

示例 3 广告软件和间谍软件。

3.9
黑客攻击
未经用户或所有者授权故意访问计算机系统

3.10
hacktivism出
于政治或社会动机的目的而进行的黑客行为(3.9)

3.11
互联网
公共领域互连网络的全球系统

[资料来源:ISO/IEC 27033-1:2015, 3.14,已修改 “the”已从术语中删除。]

3.12

网络安全

保护互联网上信息的机密性、完整性和可用性（3.11）

注1:此外,还可能涉及其他属性,例如真实性、可解释性、不可否认性和可靠性。

注 2:请参阅 ISO/IEC 27000:2018 第 3 条中有关机密性、完整性、可用性、真实性、责任性、不可否认性和可靠性的定义。

3.13

互联网服务提供商

互联网服务供应商

向用户提供 Internet 服务并使其客户能够访问 Internet 的组织
(3.11)

注 1:此外,有时也称为互联网接入提供商 (IAP)。

3.14

恶意内容

嵌入、伪装或隐藏恶意特征或功能的应用程序、文档、文件、数据或其他资源

3.15

恶意软件

恶意软件

恶意设计的软件包含可能直接或间接对用户和/或用户计算机系统造成损害的特性或功能

示例:病毒、蠕虫和木马。

3.16

组织

具有自己的职能、责任、权力和关系以实现其目标的个人或团体

注 1:在本文档中,个人不同于组织。

注 2:一般来说,政府也是一个组织。在本文件中,为清楚起见,可以将政府与其他组织分开考虑。

[资料来源:ISO 9000:2015, 3.2.1,已修改 - 条目注释 1 和条目注释 2 已被替换。]

3.17

网络钓鱼

试图通过在电子通信中伪装成值得信赖的实体来获取私人或机密信息的欺诈过程

注 1:网络钓鱼可以通过使用社会工程或技术欺骗来完成。

3.18

可能不需要的软件

欺骗性软件（3.8）,包括具有欺骗性软件特征的恶意软件（3.15)和非恶意软件

3.19

垃圾邮件

可能携带恶意内容和/或诈骗消息的未经请求的电子邮件

注 1:虽然最广泛认可的垃圾邮件形式是电子邮件垃圾邮件,但该术语也适用于其他媒体中的类似滥用行为:即时消息垃圾邮件、Usenet 新闻组垃圾邮件、网络搜索引擎垃圾邮件、博客垃圾邮件、维基垃圾邮件、手机短信垃圾邮件、互联网论坛垃圾邮件和垃圾传真传输。

[来源:ISO/IEC 27033-1:2015, 3.37,已修改 - 已添加条目注释 1。]

3.20
间谍软件
欺骗性软件(3.8),从计算机用户收集私人或机密信息

注 1:信息可以包括最常访问的网站等内容或更敏感的信息（例如密码）。

3.21
威胁
意外事件的潜在原因,可能对系统、个人或组织造成损害
(3.16)

3.22
木马
恶意软件(3.15)似乎为用户执行了所需的功能,但误导了用户其真实意图

3.23
网络钓鱼
通过伪装成值得信赖的实体来进行语音网络钓鱼,以获取私人或机密信息

注 1:语音钓鱼可以通过语音电子邮件、VoIP（IP 语音）、固定电话或移动电话进行。

3.24
水坑技术
煽动人们访问专门包含（大量)恶意软件的网站的技术

注1:水坑也称为水坑。

3.25
全球资讯网
网络
可通过网络访问的信息和服务的范围

[来源:ISO 19101-1:2014, 4.1.40]

4 缩写术语

本文档中使用了以下缩写术语。

人工智能	人工智能
应用程序编程接口	应用程序接口
易于	高级持续威胁
自带设备	带上你自己的设备
计算机紧急响应小组	计算机应急小组
分布式拒绝服务	分布式拒绝服务
数字光处理	数据丢失预防
非军事区	非军事区
域名系统	域名系统

拒绝服务	拒绝服务
EDR	端点检测和响应
文件传输协议	文件传输协议
HTTP协议	超文本传输协议

安全套接字层上的 HTTPS 超文本传输协议

ICANN 分配名称和号码的互联网公司

信息通信技术	信息和通信技术
入侵检测系统	入侵侦测系统
互联网工程任务组	互联网工程任务组
IMT	事件管理团队
物联网	物联网
知识产权	互联网协议
IPS	入侵防御系统
互联网服务供应商	互联网服务提供商
独立软件开发商	独立软件供应商
IRT	事件响应小组
信息管理系统	信息安全管理体系

OWASP 开放式 Web 应用程序安全项目

个人身份信息	个人身份信息
SDLC	软件开发生命周期
SIEM	安全信息和事件管理
中小企业	中小企业
网址	统一资源定位器
USB	通用串行总线
VPN	虚拟专用网络
万维网联盟	万维网联盟

万维网

5 互联网安全、网络安全、网络安全和网络安全之间的关系

图 1显示了互联网安全、Web 安全、网络安全和网络安全之间关系的高级视图。

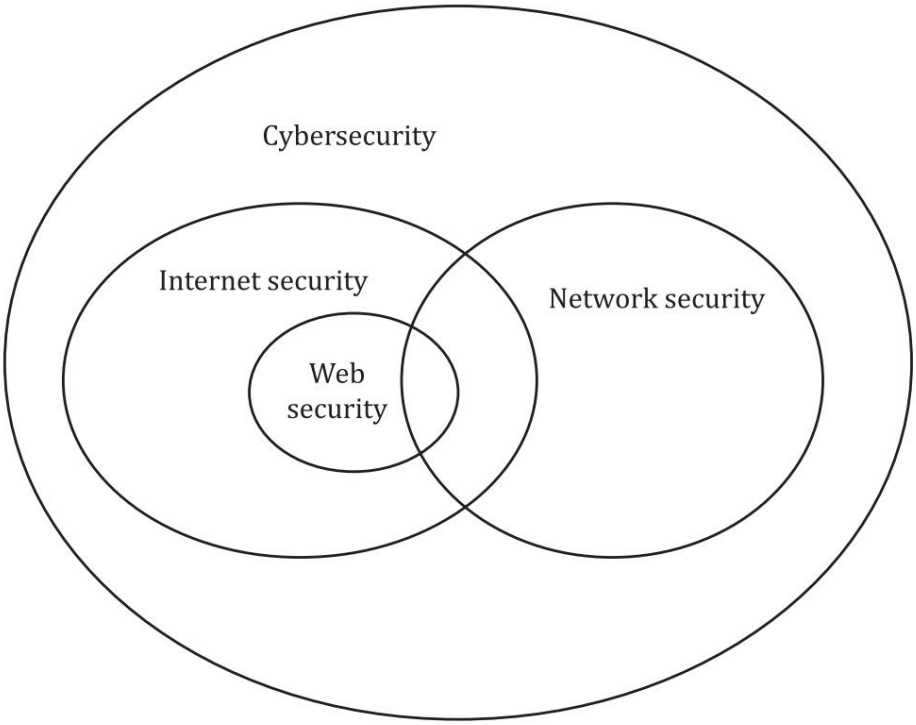

图 1　互联网安全、网络安全、网络安全和网络安全之间的关系

互联网是公共领域内相互连接的数字网络的全球系统。互联网上的信息交换也使用移动电话网络,因此移动电话网络是互联网的一部分。这个全球网络连接数十亿台服务器、计算机和其他硬件设备。每个设备都通过其与互联网的连接与任何其他设备连接。互联网创造了有利于信息共享的环境。

互联网安全关注的是保护互联网相关服务以及相关ICT系统和网络,作为网络安全的延伸。这些努力旨在减少组织、客户和其他相关利益相关者与互联网相关的安全风险。

互联网安全还确保互联网服务的可用性和可靠性。通过互联网,提供各种服务,例如文件传输服务、邮件服务或任何可以与最终用户公开共享的服务。在这种情况下,互联网安全涉及通过公共网络安全交付这些服务。

Web 是在 Internet 上共享信息的方式之一 [其他包括电子邮件、文件传输协议 (FTP) 和即时消息服务]。网络由数十亿个相互连接的数字文档组成,可以使用网络浏览器查看这些文档。网站是一组相关的网页,它们作为支持单一目的的集合而准备和维护。

Web 安全涉及万维网 (WWW) 环境中的信息安全以及通过公共网络访问的 Web 服务。 Web 服务通过使用 HTTP 协议来启用,在该协议中可以访问任何已注册的公开可用的 URL。 Web 安全还涉及用于信息交换的 HTTP 连接的安全性。

网络可以包括路由器、集线器、布线、电信控制器、关键分配中心和技术控制设备等组件。网络安全广泛涵盖组织内存在的各种网络,包括局域网、广域网、个域网和无线网络。

网络安全涉及网络的设计、实施、运行和改进,以及组织内部、组织之间、组织与用户之间与网络相关的安全风险的识别和处理。

网络安全涉及当信息在计算机、存储和网络中以数字形式存在时管理信息安全风险。许多信息安全控制、方法和技术可用于管理网络风险。

网络安全还涉及保护互联网连接系统,包括硬件、软件、程序和数据免受潜在攻击。其中许多攻击的特点是具有高度复杂性和持久性的针对性攻击和混合攻击。这些威胁可以是基于互联网的和/或由于与组织内的其他网络和系统或组织在正常业务过程中与之通信的客户和服务提供商的网络的连接而产生的威胁。

6 互联网安全概述

互联网用户的个人身份信息 (PII) 被互联网上提供的许多站点和服务捕获。这包括密切跟踪用户活动并使用人工智能 (AI) 技术提供购买、医疗保健、时间管理和许多其他反馈建议的应用服务提供商,旨在使他们的生活和任务更容易管理。许多此类网站在未经用户许可的情况下收集这些数据,并在用户不知情的情况下将这些数据提供给其他第三方以获取金钱利益。感兴趣的各方已经通过网站在互联网上建立了自己的存在,在全球范围内开展电子商务,在互联网上提供数字服务,使用公共云服务来提供服务以及使用基于网络的商业应用程序和服务。

互联网的许多用途涉及信息交换和提供与个人和 PII 无关的服务。 PII 因司法管辖区而异。此类信息和服务的安全性对于相关方而言至关重要。此外,在所谓的物联网中,作为个人设备或专用网络连接到互联网的硬件范围正在迅速增加。物联网中人工智能的自主性和应用提出了具有挑战性的互联网安全要求。

虽然互联网可以促进显着的业务成果,但始终存在许多需要管理的安全风险。重要的是要记住,互联网最初设计时并没有考虑到安全功能。组织严重依赖互联网的使用来开展业务。由于与互联网相关的信任度较低,如果没有充分控制,业务运营可能会因信息和服务的机密性、完整性和可用性丧失而面临严重的不利后果。

虽然有些人在管理自己的在线身份时非常小心,但大多数人都会上传个人资料的详细信息以与他人分享。许多网站（特别是社交网站和聊天室)上的个人资料可以由其他方下载和存储。这可能会导致创建个人数据的数字档案,该档案可能被滥用、泄露给其他方或用于二次数据收集。虽然这些数据的准确性和完整性值得怀疑,但它们与个人和组织建立了联系,而这些联系通常无法完全删除。通信、娱乐、交通、购物、金融、保险和医疗保健领域的这些发展给互联网上的利益相关方带来了新的风险。因此,风险可能与互联网隐私的丧失相关。

信息和通信技术的融合、从台式机、笔记本电脑到移动和物联网设备进入互联网的便捷性,以及个人之间个人空间的缩小,正在引起恶意行为者和犯罪组织的关注。

这些实体正在使用网络钓鱼、垃圾邮件和间谍软件等机制,并开发零日攻击、网络钓鱼、恶意网站和其他欺骗技术等攻击技术,以利用他们在互联网上发现的任何弱点。

近年来,互联网安全攻击已从为了个人名誉而进行的黑客攻击演变为有组织犯罪或网络犯罪。以前在孤立的网络安全事件中观察到的大量工具和流程现在被一起用于多重混合攻击,通常具有深远的恶意目标。

其中许多工具也可以在公共软件存储库和其他公开可用的资源中找到。攻击的目标包括人身攻击、身份盗用、金融欺诈或盗窃、黑客行动和互联网上的信息操纵。许多被盗的个人数据和客户数据也可以在暗网上获取,可以公开访问。组织,尤其是中小企业,应该了解“操纵”互联网信息的真正后果。这些安全风险是用户访问互联网时面临的网络风险。

由于互联网是一个全球公共网络,交易可以来自世界任何地方,攻击也可以。在互联网上进行的多种商业交易模式正在成为网络犯罪集团的目标。从企业对企业、企业对消费者到消费者对消费者的服务,所带来的风险本质上是复杂的。

另一个复杂性源于这样一个事实:所有利益相关方,即使他们没有恶意,对他们的需求、要求和威胁也有不同的看法,因此他们有不同的风险和控制措施来应对它们。这意味着不存在“一刀切”的解决方案。

交易或协议的构成等标准取决于各个司法管辖区的具体法律和监管环境。这些标准还取决于法律的解释以及关系中的各方如何管理其责任。通常,使用在交易或关系期间收集的数据的问题没有得到充分解决。这最终可能导致信息泄露等安全问题。

这些互联网问题带来的法律和技术挑战是深远的、全球性的。这些挑战只能通过信息安全技术界、法律界和不同地区之间的合作,采取一致的策略来应对。该战略应在国际合作框架内考虑到每个相关方的作用和现有举措。

信息通过互联网即时传播,这意味着攻击也可能即时发生。由于这些速度不容易被人的思维所理解,因此攻击总是在发生很长时间后才被发现,并且造成的损失已经是巨大的。在大多数情况下,攻击者的身份是隐藏的。因此,经常提出使用人工智能(AI)来应对攻击。

7 利害关系方

7.1 概述

互联网安全的利益相关方包括:

- 通过互联网使用服务;
- 利用互联网提供服务;
- 提供互联网的基础设施和通信能力;
- 全球协调互联网的运营;
- 制定并执行法律法规。

互联网安全的利益相关方可分为用户(7.2)、协调者和标准化组织(7.3)、政府当局(7.4)、执法机构(7.5)和互联网服务提供商(7.6)。

7.2 用户

用户是指使用互联网的个人、最终用户以及私人和公共组织。私营组织包括中小企业（SME)和大型企业。政府和其他公共机构统称为公共组织。

当个人或组织访问互联网或通过互联网提供的任何服务时，他们就成为用户。用户可以利用互联网服务、查看或收集信息。他们还可以提供应用程序空间内的某些特定信息，或者向应用程序空间内的有限成员或团体或公众开放。

用户角色可以包括但不限于以下内容：

一般互联网应用用户，或者说网络游戏玩家、即时通讯工具等一般用户
用户或网络冲浪者；

买方/卖方，参与将商品和服务放在在线拍卖和市场网站上
有兴趣的买家，反之亦然；

博主和其他内容贡献者（例如，维基百科上文章的作者），其中发布文本和多媒体信息（例如视频剪辑)以供公众或有限受众消费；

组织的成员（例如公司的员工，或其他形式的协会的成员）
公司）；

其他角色，可以无意或未经用户同意为用户分配角色。

示例1 当用户访问需要授权的站点并且有意或无意地获得访问权时，该用户可以被标记为入侵者。

示例 2 充当买方或卖方的个人可能在不知情的情况下参与销售赃物的犯罪交易或洗钱活动。

组织经常使用互联网来宣传公司和相关信息，以及营销相关产品和服务。组织还利用互联网作为其网络的一部分来发送和接收电子消息（例如电子邮件)和其他文档（例如文件传输）。

本着成为良好企业公民的原则，这些组织应将其企业责任延伸至互联网，积极确保其在互联网使用中的做法和行为不会给互联网用户社区带来进一步的安全风险。

一些积极措施包括：

通过实施和运行有效的信息安全管理体系（ISMS)进行信息安全管理（信息安全管理体系的要求见ISO/IEC 27001）；

实施基于 ISO/IEC 27002 和其他相关标准的控制，无需操作
信息安全管理体系；

安全监控和事件响应；

将安全性纳入软件开发生命周期（SDLC)的一部分，其中系统内置的安全级别应根据组织的数据关键性来确定；

通过持续的技术和流程对组织中的用户进行定期安全教育
更新并跟踪最新技术发展；和

了解并使用适当的渠道与供应商和服务提供商就使用过程中发现的安全问题进行沟通。

7.3 协调机构和标准化组织

协调机构和标准化组织（ICANN、IETF、W3C 等）制定有关互联网使用和服务提供商提供的服务的技术标准。他们向组织提供有关其在互联网上的角色和责任的建议。

7.4 政府当局

政府拥有有关国家安全、战略、军事、情报问题以及与政府和国家有关的许多其他要素的信息，而且还拥有有关个人、组织和整个社会的大量信息。

各国政府应保护本国的基础设施和信息免遭未经授权的访问和利用。利用互联网提供电子政务服务的趋势不断增长和扩大。这是发起攻击和获取上述信息的新渠道，如果成功，可能会对一个地区、其政府和社会造成严重影响。

政府当局在执法机构之间发挥协调作用，并且是在大规模网络攻击引发危机时在国家层面和企业层面传播信息和协调任何所需资源的主要协调者。这还包括 CERT 等机构和类似组织，根据具体地区的具体情况，这些机构被赋予此类职责。

政府要求为大学和高中开设网络安全教育项目，并确保建立适当的公私合作伙伴关系，并建立必要的法律结构，组织执法机构并确定其使命。

7.5 执法机构

执法机构执行法规，并要求所有利益相关方在其国家管辖范围内遵守相关法规。

7.6 互联网服务提供商

服务提供组织可以包括两类：

- 为员工和合作伙伴提供互联网接入的提供商；
- 为互联网消费者提供服务的提供商。

这些服务通过互联网上的云服务提供商等应用程序交付提供给封闭社区（例如注册用户）或公众。

如果消费者反过来通过互联网提供服务或使另一个消费者能够访问互联网，那么消费者也可以是服务提供商。

服务提供商也可以被理解为运营商或批发商，而不是接入服务的分销商和零售商。从安全角度，特别是从执法角度来看，这种区别很重要。如果分销商或零售商无法提供足够的安全性或合法访问权限，支持服务通常会默认返回给运营商或批发商。互联网服务提供商 (ISP) 可以通过监督“流量”并提供替代路由或流量控制主机来提供支持。他们还可以寻找互联网上的“危险”传输。凭借必要的法律授权和用户的授权，他们可以过滤危险内容，就像提供“沙箱”来验证传输文件是否存在恶意软件的解决方案一样。 ISP 可以在发现威胁模式时向客户发出警告。

8 互联网安全风险评估与处置

8.1 概述

ISO 31000 提供风险管理的原则和通用指南,而 ISO/IEC 27005 提供组织中信息安全风险管理的指南和流程,支持 ISO/IEC 27001 的 ISMS 要求。这些文件提供的指南和流程是建议用于解决互联网背景下的风险管理。相关方有责任定义其风险管理方法。可以在 ISO/IEC 27005 描述的框架下使用多种现有方法来进行风险评估并管理与组织使用互联网相关的风险,同时考虑相关威胁和漏洞以及互联网安全问题。

在可用资源有限的组织中,控制措施需要考虑组织安全需求和资源之间的合理性,以避免控制措施选择上的错误。控制措施选择不当可能会导致额外的风险或无效的控制措施。

8.2 威胁

威胁主体是在执行或支持攻击中发挥作用的个人或个人团体。彻底了解他们的动机（宗教、政治、经济等）、能力（知识、资金、规模等)和意图（娱乐、犯罪、间谍活动等)对于评估脆弱性和风险至关重要,因为以及控件的开发和部署。

恶意软件可能导致安全控制受到损害（例如,捕获和泄露密码）、意外泄露信息、意外更改信息、破坏信息和/或未经授权使用系统资源。恶意软件通常通过病毒、蠕虫和木马传播,并产生深远的影响。

病毒是一种可执行且可复制的程序,它将自己的代码插入到合法程序中,其目的是破坏主机（即删除文件和程序、损坏存储和操作系统）。在最简单的状态下,蠕虫是一种计算机程序,旨在通过向用户联系人列表中的所有地址发送出站消息进行自我复制并传播到其他计算机,从而耗尽系统资源。此外,就像病毒一样,蠕虫病毒可以传播可能损害其宿主的代码。此类代码被称为有效负载（例如,加密勒索软件中的文件的能力以及安装支持远程访问的系统后门）。特洛伊木马是一种伪装成或嵌入合法软件中的恶意程序,其目标与病毒和蠕虫相似,但与它们不同的是,它不会自行复制或传播。

对互联网用户个人身份信息（PII)的互联网安全威胁主要围绕身份问题,即个人信息泄露或被盗造成的。如果一个人的在线身份被盗或伪装,该人可能会被剥夺对关键服务和应用程序的访问权限。在更严重的情况下,后果可能从金融到国家级事件不等。未经授权访问个人的财务信息也可能导致个人资金被盗和欺诈。

示例 1 信用信息可以在黑市或暗网上出售,这可能会促进在线身份盗窃。

示例 2 等同于生命威胁的其他威胁示例包括网络欺凌、在线跟踪和剥削犯罪,包括剥削儿童和人口贩运。

另一个威胁是包括个人设备和自带设备 (BYOD) 在内的端点有可能成为僵尸或机器人。计算设备可能会受到损害,从而成为更大的僵尸网络的一部分。组织的在线存在和在线业务经常成为不法分子的目标,他们的目的不仅仅是恶作剧。

从更大的范围来看,支持互联网的基础设施也可以成为目标。虽然这不会永久影响互联网的功能,但会影响基础设施的可靠性和可用性,从而有助于互联网的安全。

在国家或国际层面上,互联网是特定管辖范围内非法行为猖獗的领域。由于互联网的性质,特别是定义界限和边界方面的挑战,很难规范和控制其使用方式。

犯罪分子可以合法购买有利于其目的的应用程序、服务和资源,也可以采取非法手段来保护这些资源以避免被发现和跟踪。这可能包括通过僵尸网络获取大量计算资源。

另一个威胁涉及故意修改公开信息或专有信息,或者制造虚假信息和恶作剧,如果依赖这些信息和恶作剧,可能会造成严重损害。

8.3 漏洞

脆弱性是指资产或控制中可能被威胁利用的弱点。一旦发现并解决这些弱点,制造商、软件开发商和其他技术开发商就会制作安全更新和补丁来修复这些弱点。当系统收到补丁时,会添加更新或新元素。当系统过时或不受供应商支持或未修补到最新版本时,可能会引入新的漏洞。利益相关方应对相关资产或控制权以及所涉及的威胁、威胁主体和风险有透彻的了解和了解,以便进行全面的评估。感兴趣的各方应该注意没有可用补丁的零日漏洞。

通过 Internet 访问的 Web 应用程序很容易受到各种漏洞的影响,这些漏洞是由不良设计、编写不良的代码以及构建不良的生产库和可执行文件引起的。
此类漏洞的示例包括身份验证绕过、数据库注入攻击和跨站点脚本攻击。在这些攻击中,可以操纵请求来滥用网络服务器功能。

8.4 攻击向量

攻击向量是攻击者可以访问计算机或网络服务器以传递恶意结果的路径或手段。

端口扫描器是攻击者使用的最古老但仍然非常有效的工具之一。他们扫描面向互联网的系统上的所有可用端口,以确认哪些端口是开放的。这通常是潜在攻击者在面向互联网的目标系统上执行的首要步骤之一。虽然初始攻击始终针对面向公众的系统（例如路由器、服务器、防火墙、网站等）,但攻击者也可以寻求利用驻留在连接到这些面向公众的系统的专用网络内的资产。

监听通信渠道是一种简单且容易的攻击方式。它也是最古老的之一。
复制和分析流量对于检测入口点和发起其他威胁向量非常有价值。攻击者还可以使用通信劫持（通过尾随或捎带）并在身份或凭证后面伪装自己,并在合法用户不知情的情况下付出代价。

许多互联网攻击都是使用恶意软件进行的,例如间谍软件、蠕虫和病毒。信息通常是通过网络钓鱼技术收集的。攻击可以作为单一攻击向量发生,也可以作为混合攻击或有针对性的攻击进行。这些攻击可以通过可疑网站、未经验证的下载、垃圾邮件、远程利用、零日利用和受感染的可移动媒体等传播。

用于实施攻击的其他机制的使用和复杂性不断增长,这些机制是基于社交网站和在合法网站上使用损坏的文件的机制。合法网站也可能被黑客入侵并损坏其部分文件,并被用作实施攻击的手段。

人们倾向于隐含地信任经常访问的网站。攻击者可以应用水坑

通过感染经常访问的网站来危害特定最终用户组的技术。除了人类攻击者发起的攻击外,受恶意软件感染的计算机还会对周围连接的计算机发起各种攻击。

随着通常用于共享数字音乐、视频、照片等文件的点对点应用程序的激增,攻击者在如何使用交换的文件作为木马来伪装自己及其恶意代码方面变得越来越熟练。他们的攻击。一旦攻击者通过身份盗窃将自己伪装成合法联系人,攻击者就可以与其他人接触,并为发起各种类型的攻击开辟了新的途径。

另一种技术是 IP 欺骗,其中攻击者操纵与其消息关联的 IP 地址,试图将其伪装成已知的可信源,从而获得对系统的未经授权的访问。

攻击者并不总是使用相同的攻击向量。它使用多个向量并经常更改它们。有些攻击的隐藏程度很高,以至于用户无法检测到,但为时已晚。防御者应该考虑这一点,并寻求针对多个向量的防御,而不仅仅是那些已经用于对抗它们的向量。

物联网设备、智能手机等可以连接到互联网。如果这些设备在连接到组织的网络时没有得到充分的控制,就像任何其他连接互联网的设备一样,它们可以充当额外的攻击媒介。

高级持续性威胁 (APT) 是一种攻击方法,其目标是长期窃取信息,攻击者可以持续访问组织的网络、不被发现、横向移动、查看、学习并留在网络中。

另一种古老的攻击方法是暴力破解。这使用反复试验来猜测登录凭据、加密密钥,查找隐藏的网页,攻击者通过所有可能的组合进行操作,希望能够正确猜测以获取对组织网络和信息的访问权限。

9 互联网安全指南

9.1 概述

相关方可以通过考虑适用于其资产的威胁来评估风险。此分析可以帮助选择控制措施来应对风险并将其降低到可接受的水平。

实施控制措施是为了减少此类风险的可能性或后果,并满足相关方的安全要求（直接或通过向其他方提供指示间接地）。

实施控制措施后,漏洞可能仍然存在。此类漏洞可能被威胁代理利用。考虑到其他限制,利益相关方寻求将风险最小化。利益相关方应确信,在允许资产遭受特定威胁之前,控制措施足以应对资产威胁。如果相关方不具备评估控制措施各个方面的能力,他们可以寻求外部组织对控制措施进行评估。

应对互联网安全风险的有效方法是多种策略的结合,并考虑到各个利益相关方。

这些策略包括:

- 行业特定方法,与所有相关方合作确定和解决
  互联网问题和风险;

- 广泛的消费者和员工教育,为如何识别和解决组织内以及互联网社区中的特定互联网风险提供值得信赖的资源

  用户;

创新技术解决方案,帮助保护消费者免受已知的基于互联网的攻击,
保持最新状态并为新的利用做好准备;

更新立法和法规,使司法管辖区能够伸张正义。

9.2 互联网安全控制

9.2.1 概述

大多数组织将互联网用于各种目的,从网上冲浪、博客、社交网络和访问公共云服务,到信息共享和开展电子商务业务。这涉及在执行在线交易时共享包括个人信息在内的机密商业信息。互联网作为公共网络很容易受到某些独特的威胁。如果不加以解决,这些威胁将导致难以管理的攻击。

组织应制定政策、程序和响应能力,以便:

a) 定义人员可接受的互联网使用规则;

b) 定义哪些服务可以通过互联网公开;

c) 识别威胁、漏洞、攻击媒介及其相关风险;

d) 定义互联网不同用户的角色和责任;

e) 提高用户对互联网使用安全做法的认识;

f) 明确处理互联网安全问题的责任部门;

g) 建立网络安全事件响应机制;

h) 进行安全演习,测试针对来自以下来源的攻击的响应机制:
互联网。

根据风险评估,人们可以发现各种相关的互联网安全风险,这些风险可以通过各种控制措施来解决,如下所述。

9.2.2 互联网安全政策

组织应根据安全目标制定并发布有关人员和其他相关方使用互联网的政策。这决定了使用哪些互联网服务、谁有权使用这些服务以及安全目标是什么。本政策指导安全连接和使用互联网的所有其他准则。

互联网安全政策应由管理层制定、批准、发布、传达给相关人员、承包商和外部各方,并得到相关人员、承包商和外部各方的认可。互联网安全政策应当规定有权访问互联网的人员、可以查看的内容、禁止的互联网行为等。应为与互联网有关的所有活动以及适用于互联网安全的所有具体控制措施的设计、批准、实施、操作和监控分配职责。

ISO/IEC 27002 提供了有关互联网安全政策的进一步指导。

9.2.3 访问控制

访问控制不仅包括用户的访问权限,还包括其他实体(例如设备、应用程序或自动化流程)的访问权限。因此,应根据业务和安全规则建立的角色和权限对每个连接进行身份验证,对每个活动进行适当授权,并且应为每个实体分配最低特权。这增强了信息和资产访问的可追溯性,并减少匿名性以提高安全性。

应根据业务和信息价值建立和实施控制对信息和资产、与互联网相关的其他资产和信息处理设施的物理和逻辑访问的规则。有关访问基本信息和资产、与信息和信息处理设施相关的其他资产的规则应符合既定的访问控制政策和信息分类政策。

帐户应仅限于因其工作角色或职能而获得授权的用户。每个用户都应该有单独的帐户，并且不应共享这些帐户，也不应为多个帐户使用相同的密码。

应根据组织的访问控制政策和程序来配置、审查、调整、修改和删除对信息、系统、应用程序和服务的访问权限。特权访问权限的分配和使用应受到限制和控制。应根据信息访问限制和相关访问控制规则实施安全认证技术和程序。应建立密码管理系统来管理和支持密码创建过程及其质量。

直接连接到互联网的信息系统（例如防火墙基础设施、网络周边设备等）可以具有一个或多个能够超越系统和应用程序控制的特权实用程序。如果攻击者能够访问任何系统，那么这些特权实用程序如果控制不当，可能会导致攻击者获得特权访问。

这些程序应由组织充分控制，以便入侵者无法访问此类特权实用程序并覆盖系统和应用程序控制。有效的访问管理应包括：

定期审查所有访问权；

定期审查管理日志。

ISO/IEC 27002 和 ISO/IEC 29146 提供了有关访问管理的进一步指导。

9.2.4 教育、意识和培训

组织人员（包括高层管理人员、系统管理员、IT 人员和特权用户等）应定期了解主要威胁（例如网络钓鱼和网络钓鱼）的最新信息以及预防威胁和应对不当行动时应采取的措施。

互联网上每天都会出现许多新的威胁，并且不断发展并变得更加隐蔽和复杂。在实施控制措施来应对攻击时，用户可能不知道自己是新的或更复杂的攻击的受害者。

组织应使用各种格式（例如电子邮件通信、在线培训和通过内联网发送消息）定期为人员提供意识和培训材料，以告知人员在线威胁以及可接受的使用和报告事件的义务。

这提供了一定程度的理解并引起他们的注意以保护自己和组织。

ISO/IEC 27002 提供了有关教育、意识和培训的进一步指导。

9.2.5 安全事件管理

互联网上的安全事件包括对面向互联网的组织资源以及面向互联网资源背后的服务器、数据库和应用程序的各种网络攻击。安全事件可以从互联网上的任何地方触发。有时，携带攻击的主机可能是受感染的主机。有些事件本质上可能很复杂，需要特殊技能才能做出充分反应。事件通常跨越国家、地理和组织的界限，信息流动的速度和事件发生的变化往往给响应个人和组织的行动时间带来限制。

应建立事件管理团队（IMT)和支持事件响应团队（IRT），为组织提供评估、响应此类事件并从中学习的能力。事件响应程序应考虑通过人为或自动方式检测和报告安全事件的发生，例如潜在和实际事件。组织实施的监控工具可以检测并发送安全事件以进行事件响应。威胁情报是有关威胁和威胁行为者的信息，有助于减轻网络空间中的有害事件。信息安全人员应持续扫描社交媒体情报、人类情报、技术情报或来自深网和暗网的情报等威胁情报源，收集信息并进行分析。

应建立支持信息共享和协调的技术解决方案，以帮助准备和响应安全事件和网络事件。这是组织应作为其安全控制的一部分采取的重要步骤。这样的解决方案应涉及安全、有效、可靠和高效的信息共享和协调。

与互联网安全有关的事件应由组织的指定联系人和其他相关人员或利益相关方做出回应。在实施事件管理程序时，应考虑在规定的时间范围内向相关利益方报告事件的任何外部要求（例如，在规定的时间范围内向监管机构报告事件的要求）。组织应与相关法律、监管和监督机构建立并保持联系。这些组织还应与特殊利益团体和其他专业安全论坛和专业协会保持联系。

互联网安全相关各方之间需要高效、有效的信息共享、协调和事件处理。这种合作应该以安全可靠的方式进行，同时保护相关个人的隐私。许多相关方可能居住在不同的地理位置和时区，并且可能受到不同的监管要求的管辖。

信息共享和协作包括：

- 建立信任的考虑因素的关键要素；
- 协作以及信息交换和共享的必要流程；
- 不同感兴趣的系统集成和互操作性的技术要求
  派对。

使用互联网的组织应定义并应用信息的识别、收集、获取和保存程序，这些信息可以在发生安全事件时作为证据。

如果根据监控日志和其他数字证据证明事件源自另一个国家，预计将以适当的国家法院或国际当局可接受的方式收集证据。

在发生安全事件时，数字证据可以超越组织或管辖范围。
在这种情况下，应确保组织有权收集所需的信息作为未来行动方案的数字证据。计算机时钟的正确设置对于确保审计日志的准确性非常重要，审计日志可用于在发生任何来自互联网的攻击时进行调查，或作为可能的法律诉讼的证据。

从面向互联网的系统的安全事件评估中获得的信息应用于识别重复发生或相关的事件，以便规划和实施变更，以减少未来类似事件的可能性或影响。可以根据安全事件的评估重新配置IPS和SIEM等工具，并启动相关的政策修订以防止未来的事件发生。

ISO/IEC 27002 和 ISO/IEC 27035 系列提供了有关事件管理的进一步指导。

9.2.6 资产管理

应确定包含关键信息和应用程序的 ICT 组件。传统上,组织需要知道其资产的实际位置,以便充分保护它们。组织不仅应在其控制范围内保留最新 ICT 资产的清单,还应维护信息资产登记册,记录其信息的处理、存储、传输位置,无论是在其内部网络上还是使用云/互联网。基于托管解决方案。通过这种方式,组织可以管理其信息(无论其位于何处)的风险,并就该信息是否适合存储在组织的控制环境之外做出基于风险的决策。同样,对于网络组件,组织应该知道敏感资产位于潜在攻击者入口点的位置。这可以是通过防火墙的官方互联网访问以及与设备(例如智能手机、物联网)的所有其他连接。组织还应确定用于访问敏感 ICT 资产或在组织网络内传输敏感信息的关键路径。这些路径不应被入侵者看到、访问或监视。如果没有这些知识,就不可能对网络进行充分的隔离。该清单应采用网络架构(功能的位置)和基础设施的形式,两者都清楚地指示互联网(所有互连网络)的入口/连接点。

应确定、记录和实施资产、与互联网相关的其他资产和相关处理设施的可接受使用和处理程序的规则。

组织应制定并使用程序来评估持有和转让信息和 ICT 资产的重要性。这将使组织能够清楚地确定应保护什么以及在通用策略和网络安全方面应保护的级别。

ISO/IEC 27002 提供了有关资产管理的进一步指导。

9.2.7 供应商管理

应确定并实施流程和程序来管理与使用供应商相关的互联网安全风险。应根据供应商的类型和相关风险,建立所有相关的信息安全要求并与每个供应商达成一致。与 ICT 供应商及其存储、利用或可以访问的信息相关的风险管理是准备合同以确保持续实现组织的信息安全目标的关键。

应与互联网相关供应商(例如互联网服务提供商和云服务提供商)建立协议并记录在案,以确保组织和供应商之间对双方履行相关信息安全要求的义务有明确的了解。组织应与 ISP、电信服务提供商、云服务提供商和合作伙伴建立开放的合作伙伴关系,以通知/警告检测到的传入威胁。应确定并定期监控互联网服务提供商以安全方式管理约定服务的能力。预计组织和服务提供商就审核权达成协议。

对于通过 Internet 访问并由组织订阅的云服务,组织应与云服务提供商审查并协商云服务协议。

组织应进行相关风险评估,以识别与使用云服务相关的风险,并在协议期限内管理风险。云服务协议应满足组织的机密性、完整性、可用性和 PII 处理要求。对于组织无法协商协议条款的任何云服务,组织应该睁大眼睛签订协议,了解使用该服务的风险以及如何在协议期限内管理这些风险。

基于云的工具(例如网络会议工具、网络聊天工具和云存储工具)如果具有可被不良行为者利用的固有安全错误,就会给组织带来风险,因此组织建立使用安全控制非常重要这些基于云的工具。

可以考虑将以下内容纳入协议中,以满足已确定的要求
互联网安全要求:

a) 法律和监管要求,包括 ISP 端的信息保护要求,例如免受 DDoS 和其他攻击的保护;

b) 合同各方有义务实施一套商定的控制措施,包括访问控制、网络和系统监控、报告和审计;以及供应商遵守组织安全要求的义务;

c) 事件管理要求和程序(特别是事件补救期间的通知和协作);

d) 对供应商服务的监控、审查和变更管理,以确保协议的信息安全条款和条件得到遵守,并允许监控服务绩效水平,以验证对协议的遵守情况,监控供应商所做的变更并监控供应商服务的变化。

ISO/IEC 27002、ISO/IEC 27036 系列、ISO/IEC TR 23187 和 ISO/IEC 27017 提供了与供应商相关的进一步指南。

9.2.8 互联网上的业务连续性

一些业务活动(例如基于互联网的贸易和其他电子商务活动)取决于组织内的互联网基础设施。不良行为者的 DoS 和 DDoS 攻击、外围设备故障或 ISP 端的任何中断都可能导致互联网服务中断。 ISP 端的不良行为者也可能进行 DoS 和 DDoS 攻击,这可能导致互联网主干网完全中断。信息处理设施应具有足够的冗余以满足可用性要求。

互联网基础设施中的任何中断都会对组织构成连续性风险,应由组织解决。组织应计划从不同的 ISP 采购互联网服务,以实现基本的连续性措施。组织应部署安全措施以避免中断,例如用于网络设备连续性的反 DDoS 措施。组织还可以要求各自的 ISP 在 ISP 网络内部署反 DDoS 措施。无论连续性服务如何,组织都应继续考虑任何解决方案中的信息安全,即使处于业务连续性模式下也是如此。

ISO/IEC 27002、ISO 22301 和 ISO/IEC 27031 提供了与 ICT 连续性相关的进一步指导。

9.2.9 互联网隐私保护

大多数服务提供商控制或处理 PII。当这些信息用于与数据主体利益不同的目的时,就会引发隐私问题。托管服务提供商在其网络和数据中心处理 PII,作为其业务服务的一部分。这些服务(包括网站和其他在线应用程序)通常通过将订户托管给其他消费者(例如小型企业和最终用户)来重新打包和转售,并通过互联网进行访问。

如果托管订户设置不安全的服务器,或在其网站或应用程序中托管恶意内容,消费者的安全(包括此类在线应用程序存储的 PII)将受到不利影响。因此,重要的是,服务至少要遵守涵盖用户隐私要求的最低协议条款,以满足最佳实践标准。除了面向互联网的网站或应用程序的数据保护和个人隐私规定之外,服务提供商还应要求在其网络上托管的此类网站或应用程序在上线之前在应用程序级别实施一组最佳实践安全控制。在注册互联网服务之前,组织应进行隐私影响评估(PIA),以确定可以使用、收集、处理、存储或传输的个人信息以及相关的隐私风险,以确定它们是否可以接受组织并相应地管理这些。这不仅包括收集客户数据以提供服务,还包括收集元数据,例如个人浏览的 IP 地址或地理位置数据

网站。组织应在其网站上发布隐私声明,以明确告知所有用户与组织在线服务交互的要求。应根据组织的访问控制策略和业务要求使用数据脱敏,并考虑法律要求。 DLP 措施应应用于处理、存储或传输敏感信息的系统和网络。某些互联网浏览器中的技术功能允许用户更改隐私设置。

ISO/IEC 27002、ISO/IEC 27701、ISO/IEC 29100 和 ISO/IEC 27018 提供了与隐私相关的进一步指南。

9.2.10 漏洞管理

应及时获取有关正在使用的ICT系统的漏洞的信息。应评估组织面临此类漏洞的风险,并采取适当的措施来解决相关风险。应建立、记录、实施、监控和审查配置,包括硬件、软件、服务和网络的安全配置。

提供技术产品（防火墙、IDS、IPS 等)和服务（网络服务、VoIP 服务、托管安全服务等)的组织应一致有效地实施措施,以识别、处理和披露其提供的产品和服务的漏洞。根据产品和服务供应商披露的漏洞,采取适当的保护措施来解决漏洞。

随着互联网上恶意软件的不断增加,服务提供组织可以接收与恶意软件和间谍软件感染以及其他安全问题相关的报告。此类信息对于相关供应商评估恶意软件感染的风险并提供必要工具的更新以确保可以有效删除或禁用检测到的任何新恶意软件或间谍软件非常重要且有用。在这方面,组织应与安全供应商建立联系,并向供应商提交相关报告和恶意软件样本以供跟进,特别是在流行率似乎激增的情况下。大多数供应商都会维护一个电子邮件列表,用于接收此类报告或样本以进行分析和跟进。

在计算设备上不受控制地安装软件可能会导致引入漏洞。
组织应针对用户可以安装的软件类型定义并执行严格的策略。
当软件补丁可以帮助消除或减少安全漏洞时,就应该应用它们。

供应商提供的用于互联网操作系统的软件应保持在供应商支持的水平。随着时间的推移,软件供应商不再支持旧版本的软件。

组织应考虑在操作系统中使用时依赖不受支持的软件（包括开源软件)的风险。操作系统中使用的开源软件应维护到最新的适当版本的软件。

其他漏洞缓解措施包括:

a) 改变操作实践;

b) 重新配置技术系统;

c) 通过管理互联网访问来规避风险;

d) 培训员工和用户;

e) 采用纵深防御措施,即当一个控制失败时,还有另一个独立的控制
继续防守的方法到位;

f) 系统安全测试、安全 SDLC 以及补丁测试、部署前更新。

ISO/IEC 27002、ISO/IEC 30111 和 ISO/IEC 29147 提供了与漏洞管理相关的进一步指导。

9.2.11 网络管理

减少连接到互联网的资产的暴露可以降低与未经授权的访问、篡改或损坏相关的风险。应实施控制措施以确保连接到互联网的信息的安全并保护连接的服务免受未经授权的访问。应建立控制措施来保护通过互联网传输的数据的机密性和完整性,并保护连接的系统和应用程序。应限制可连接到互联网的系统,并在允许的情况下进行身份验证。与组织的互联网基础设施相关的网络设备和系统的日志记录和监控应用于记录和检测可能影响互联网安全或与之相关的操作。组织应考虑通过将连接到 Internet 的系统与其他组织网络（如专用网络和 DMZ)隔离来管理连接到 Internet 的系统的安全性。该隔离网络的边界应明确定义,并应使用网关（例如防火墙、过滤路由器)进行控制。

网络安全实施应考虑以下因素：

确保组织的网络和互联网之间有一个受监控且可靠的接口,这还确保对所有实体（而不仅仅是授权人员)的访问控制。在授予进出内部基础设施的访问权限之前,还应控制信息和应用程序。

通过创建具有适当访问控制的孤岛或集群,构建内部网络,将高度关键的资产与通用资产隔离。确保子网具有过滤路由器和嵌入式子网,以避免直接到达关键资产。

监控和分析内部流量以检测和阻止非法活动。

确保互联网及其服务的访问和使用（包括与人员的沟通）在物理设施之外工作)被保留。

确保内部网络与内部边界保护充分隔离,以将关键或关键组件与入口点隔离,并易于访问内部传输通道。

关于互联网的使用和通过互联网访问的服务应制定规则,至少涵盖以下方面：

a) 用户可以通过互联网访问的网络服务以及此类服务的授权程序；

b) 保护互联网访问的网络管理和技术控制及程序互联网上的连接和网络服务；

c) 用于访问互联网和通过互联网提供服务的方式（例如 HTTPS、VPN）；

d) 监控通过互联网访问的服务（例如带宽监控、SIEM）。

防火墙是关键的网络外围设备,组织应考虑能够更好地应对基于 Internet 的攻击的防火墙技术。该设备的目的是提供针对来自互联网的威胁的保护,并防止专有信息不受控制地传输到互联网。路由器技术可以与内置功能或附加模块一起部署,以增强网络安全性,并可以解决 DoS 和 DDoS 攻击等网络风险。

基于网络的 IDS 和基于网络的 IPS 技术可以与人工智能和机器学习一起部署,以应对基于互联网的高级攻击,包括具有已知签名模式和行为的攻击。根据网络设置,组织可以考虑配备内置各种网络安全模块的网络设备,例如防火墙、IPS、DLP 以及针对 DNS 的攻击防护。

ISO/IEC 27002 和 ISO/IEC 27033 系列提供了有关网络安全的进一步指导。

9.2.12 防范恶意软件

反恶意软件软件扫描数据和程序以识别与恶意软件相关的可疑模式。为了能够检测新的恶意代码,确保扫描软件始终保持最新（最好是每日更新)非常重要。

鉴于新恶意软件有可能以零日漏洞为目标,因此存在可以识别已知变体的软件。这包括可以识别潜在攻击模式的技术。虽然并非万无一失,但该软件确实提供了比不使用它更高级别的保护。一些流行的操作系统具有一些嵌入式功能来防御常见的恶意软件,但仍应补充反恶意软件技术以适应更高风险的环境。

反恶意软件实施应扩展到保护不需要的互联网流量和交换（双向）,因为用户通常在不知情的情况下接收和发送恶意软件。应实施预防、检测、纠正和恢复措施来防范恶意软件,并结合适当的用户意识。

组织应考虑以下指导：

a) 在互联网网关上使用反恶意软件软件,扫描进出互联网的所有流量,包括授权使用的所有网络协议；

b) 在所有客户端系统上使用反恶意软件软件,特别是那些用于访问互联网的系统
雇员；

c) 扫描文件、电子邮件、即时通讯附件、网页和外部链接是否存在病毒,
勒索软件、木马和其他形式的恶意软件；

d) 阻止可疑的弹出窗口、网络广告、已知或可疑的恶意网站,以及使用阻止列表来提供未经授权的服务,例如聊天频道或网络邮件服务；

e) 让用户意识到在处理恶意软件时存在更大的风险
通过外部链接的外部各方；

f) 验证与恶意软件相关的准确信息是否来自合格且信誉良好的来源（例如可靠的互联网站点或反恶意软件软件供应商）；

g) 对所有允许向互联网传输数据的服务进行记录和监控；

h) 限制使用未经授权的服务来传输大量数据；

i) 实施针对非授权协议的过滤器,例如点对点网络协议；

j) 根据漏洞严重性在时间范围内修补已知系统漏洞,重点关注所有接收互联网流量的系统；

k) 配置通过互联网访问的系统和应用程序,以禁用不支持的功能
必要的（例如宏）；

l) 制定适当的恶意软件攻击恢复计划,包括所有必要的数据和软件备份（包括在线和离线备份)和恢复安排。

ISO/IEC 27002 提供了有关恶意软件防护的进一步指导。

9.2.13 变更管理

应建立变更管理政策和流程,以确保组织更轻松地推出 IT 基础设施变更、管理 IT 系统和应用程序变更,以防止意外中断、数据损坏或丢失。组织应将 Internet 上托管的系统的与 Internet 安全相关的更改纳入其变更管理流程。这些流程帮助组织请求、优先排序、授权、批准、安排

并实施任何更改。变更管理政策包括系统管理员的职责和义务、导入软件和文件、访问控制等的声明。网络组件或结构的所有更改（修改、移动、删除或添加）都应进行管理，以使架构和基础设施图纸保持最新。

ISO/IEC 27002 提供了有关变更管理的进一步指导。

9.2.14 确定适用的法律和合规要求

互联网越来越多地用作部署许多在线交易服务的平台。可能存在关于保护交易细节的机密性、完整性和可用性的数据安全、网络安全和隐私法律法规。

银行交易、支付渠道、基于移动应用程序的交易和其他电子商务活动通常由于涉及数字形式的货币而受到监管。所有信息安全和网络安全相关的法律、法规、监管和合同要求以及组织满足这些要求的方法都应予以识别、记录并保持最新。

根据法律、法规、监管、合同和业务要求，通过互联网访问的在线系统上维护的记录应受到保护，防止丢失、破坏、伪造、未经授权的访问和未经授权的发布。可能需要记录作为组织在法定或监管规则范围内运作的证据，以确保防范潜在的民事或刑事诉讼或向利益相关方确认组织的财务状况。

ISO/IEC 27002 提供了有关立法和合规性要求的进一步指导。

9.2.15 密码学的使用

密码学是确保传输信息受到保护并防止流量分析的方法之一。虚拟专用网络 (VPN) 是一个简单的解决方案。密码学有一些与加密和解密密钥的管理以及密码设备的管理相关的限制，这些限制应被视为机密和关键。

应当使用密码学来保护通过互联网传输的信息的机密性、真实性和/或完整性。 VPN 和 HTTPS（安全超文本传输协议）的实现使用加密技术来实现安全连接。应根据最佳实践选择加密算法、密钥长度和使用实践。适当的密钥管理需要用于生成、存储、归档、检索、分发、退役和销毁加密密钥的安全流程。

应保护所有加密密钥免遭修改和丢失。此外，秘密和私钥需要防止未经授权的使用和泄露。用于生成、存储和归档密钥的设备应在相关时受到物理保护。使用密码技术时，应记住，不同的法规和国家限制可能适用于密码技术的使用和加密信息的跨境流动问题。

ISO/IEC 27002 提供了有关密码学使用的进一步指导。

9.2.16 面向互联网的应用程序的应用程序安全

作为互联网基础设施一部分的系统可以采用新技术。应分析新技术的安全风险，并根据已知的攻击模式审查设计。设计系统时应嵌入安全性。还应定期审查这些系统，以确保它们在应对任何新的潜在威胁方面保持最新状态，并保持适用于所应用的技术和解决方案的进步。

组织应采用安全工程原则，包括实施安全开发生命周期，以识别和减轻正在开发的产品和解决方案中的风险。这应该考虑威胁建模、用户身份验证技术、供应链组件、安全会话控制和数据验证、清理和面向安全的设计审查，以帮助识别

面向互联网的系统上的安全漏洞。面向互联网的应用程序的应用程序代码最好从安全角度进行设计，基于这样的假设：它总是受到错误或恶意事件的攻击。

组织应制定安全和适当使用互联网资源的规则，包括对不良或不适当的网站和基于网络的应用程序的任何限制，并相应地通知其人员。这会阻止人员尝试访问此类站点。规则应保持最新。此类网站可能包含非法信息、病毒和网络钓鱼材料。

限制不良或不适当网站的技术是阻止相关网站的 IP 地址或域。某些浏览器和反恶意软件技术可以自动执行此操作，也可以进行配置以执行此操作。

应遵循安全编码标准来设计和开发应用程序。如果应用程序所有者可以通过直接远程访问服务器来访问脚本，那么原则上攻击者也可以。应配置 Web 服务器以防止在这种情况下进行目录浏览。 OWASP 指南 [23, 24]可以作为安全应用程序设计和测试的有用参考。

组织应记录代码行为，并评估该行为是否属于可被视为间谍软件或欺骗性软件的潜在领域。在后一种情况下，组织应聘请具有适当资格的评估员来评估代码是否符合反间谍软件供应商遵循最佳实践的客观标准。这可以确保组织为最终用户提供的软件工具不会被反间谍软件供应商标记为间谍软件。许多反间谍软件供应商公布了他们对软件进行评级的标准。

组织应该对其二进制文件实施数字代码签名，以便反恶意软件和反间谍软件供应商可以轻松确定文件的所有者。由 ISV 始终使用包括数字代码签名在内的最佳实践生产的软件可以归类为可能是安全的。如果组织发现有助于减少间谍软件或恶意软件问题的有用软件技术，则组织应考虑与供应商合作并使其广泛可用。

对于通过互联网处理交易的应用程序，应考虑以下因素：

维护机密性和完整性所需的保护级别要求
交易明细；

通过适当的安全控制（例如加密传输路径、数字认证）在互联网上传输交易细节；

- 在任何可公开访问的环境之外存储交易详细信息并确保存储
媒体无法直接从互联网访问；

针对攻击的弹性要求，其中可以包括保护所涉及的应用服务器或确保提供服务所需的网络互连的可用性的要求；

如果需要高度依赖软件产品的安全性，则应根据 ISO/IEC 15408 系列中所述的通用标准方案对产品进行独立验证。

安全测试应该是系统或组件暴露在互联网之前测试的一个组成部分。组织可以利用自动化工具，例如代码分析工具和漏洞扫描器，并应在系统在互联网上运行之前验证安全相关缺陷的修复情况。

安全测试应包括以下测试：

a) 安全功能，例如用户身份验证、访问限制、API 的安全使用和使用
密码学；

b) 安全配置,包括操作系统、防火墙和其他安全组件的配置。

ISO/IEC 15408 系列提供了应用保证指南。 ISO/IEC 27002 和 ISO/IEC 27034 系列提供了与应用程序安全相关的指南。

9.2.17 端点设备管理

端点设备（例如物联网设备、USB 设备、BYOD）上存储、处理或访问的信息应受到保护。应适当控制在安全区域携带和使用端点设备。应制定并实施端点设备管理的安全策略。该策略应包括设备防火墙的管理、电子邮件特定的过滤工具、互联网安全和过滤、移动设备管理和安全工具、加密和入侵检测工具。

端点安全变得更加重要,因为端点正在移出组织边界,并且用户可以使用 Internet 访问组织网络内的云和资源。应立即采取行动来应对端点的妥协,以阻止攻击者并限制进一步的损害。组织应在端点部署技术能力,以检测来自未知来源和不良行为者的任何不良流量,并做出响应。此类技术也称为端点检测和响应 (EDR) 技术。组织应该有一种机制来确保适用于最终用户系统和设备的所有组织安全策略始终处于启用状态。此类技术应确保最终用户无法禁用或绕过其端点上安装的安全功能。

端点的丢失或损坏可能会对端点（包括移动设备）上驻留的数据造成重大风险。组织应该部署技术来确保他们可以跟踪这些设备,并且在设备丢失或损坏的情况下,他们应该能够在数据被不良行为者窃取之前远程擦除设备的内容。

ISO/IEC 27002 提供了有关端点设备管理的进一步指导。

9.2.18 监控

应生成、保护、保存和分析记录活动、异常、故障和其他相关事件的日志。应保护日志并将其保存在安全位置以进行日志分析和审计。
一些法规要求将日志存储一段时间。应监控面向互联网的网络、系统和应用程序的异常行为,并采取适当的措施来评估潜在的信息安全事件。

ISO/IEC 27002 提供了有关监控的进一步指导。

附录A
（资料性）

本文件与 ISO/IEC 27002 之间的交叉引用

表 A.1显示了本文件9.2中引用的互联网安全控制措施与 ISO/IEC 27002 中包含的控制措施之间的对应关系。每列包含相关的子条款编号和副标题。

表 A.1　互联网安全控制之间的映射

ISO/IEC 27032	ISO/IEC 27002:2022
9.2.2互联网安全策略	5.1 信息安全政策 5.4 管理职责
9.2.3访问控制	5.15 访问控制 5.16 身份管理 5.18 访问权限 8.2 特权访问权限 8.18 特权实用程序的使用
9.2.4教育、意识和培训	6.3 信息安全意识、教育和培训
9.2.5安全事件管理	5.7 威胁情报 5.24 信息安全事件管理规划和准备 5.25 信息安全事件评估与决策 5.26 信息安全事件响应 5.27 从信息安全事件中吸取教训 5.28 证据收集 6.8 信息安全事件报告
9.2.6资产管理	5.9 信息和其他相关资产的清单 5.10 信息和其他相关资产的可接受使用 5.11 资产返还 5.12 信息分类
9.2.7供应商管理	5.19 供应商关系中的信息安全 5.20 解决供应商协议中的信息安全问题 5.21 管理ICT供应链中的信息安全 5.22 供应商服务的监控、审查和变更管理 5.23 使用云服务的信息安全

表 A.1 （续）

ISO/IEC 27032	ISO/IEC 27002:2022
9.2.8互联网上的业务连续性	5.29 中断期间的信息安全 5.30 ICT 为业务连续性做好准备 8.13 信息备份 8.14 信息处理设施的冗余
9.2.9互联网隐私保护	5.34 隐私和 PII 保护 8.11 数据屏蔽
9.2.10漏洞管理	8.8 技术漏洞管理 8.9 配置管理 8.19 在操作系统上安装软件
9.2.11网络管理	8.16 监测活动 8.20 网络安全 8.21 网络服务的安全 8.22 网络隔离
9.2.12防范恶意软件9.2.13变更管理	8.7 防范恶意软件
9.2.14确定适用的法律和合规	8.32 变更管理
性要求	5.28 证据收集 5.31 法律、法规、监管和合同要求 5.33 记录的保护
9.2.15加密技术的使用9.2.16	8.24 密码学的使用
面向互联网的应用程序的应用程序安全	8.23 网页过滤 8.24 密码学的使用 8.25 安全开发生命周期 8.26 应用安全要求 8.27 安全系统架构和工程原理 8.28 安全编码 8.29 开发和验收中的安全测试
9.2.17端点设备管理	8.1 用户端点设备 8.9 配置管理
9.2.18监控	8.15 日志记录 8.16 监测活动

参考书目

[1] ISO 9000:2015,质量管理体系 基础知识和词汇

[2] ISO/IEC 15408（所有部分）

[3] ISO 19101-1:2014,地理信息 参考模型 第 1 部分:基础知识

[4] ISO 22301:2019,安全性和弹性 业务连续性管理系统
要求

[5] ISO/IEC/TR 23187:2020,信息技术 云计算 与云交互
服务合作伙伴 (CSN)

[6] ISO/IEC 27001:2022,信息安全、网络安全和隐私保护 信息安全管理体系 要求

[7] ISO/IEC 27002:2022,信息安全、网络安全和隐私保护 信息安全控制

[8] ISO/IEC 27005:2022,信息安全、网络安全和隐私保护 - 管理信息安全风险指南

[9] ISO/IEC 27017:2015,信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实践规范

[10] ISO/IEC 27018:2019,信息技术 安全技术 在充当 PII 处理器的公共云中保护个人身份信息 (PII) 的实践守则

[11] ISO/IEC 27031:2011,信息技术 安全技术 信息指南
和通信技术为业务连续性做好准备

[12] ISO/IEC 27033（所有部分）,信息技术 安全技术 网络安全

[13] ISO/IEC 27034（所有部分）,信息技术 应用程序安全

[14] ISO/IEC 27035（所有部分）,信息技术 安全技术 信息安全
事件管理

[15] ISO/IEC 27036（所有部分）,网络安全 供应商关系

[16] ISO/IEC/TS 27100:2020,信息技术 网络安全 概述和概念

[17] ISO/IEC 27701:2019,安全技术 ISO/IEC 27001 和 ISO/IEC 27002 的扩展
隐私信息管理 要求和指南

[18] ISO/IEC 29100:2011,信息技术 安全技术 隐私框架

[19] ISO/IEC 29146:2016,信息技术 安全技术 访问框架
管理

[20] ISO/IEC 29147:2018,信息技术 安全技术 漏洞披露

[21] ISO/IEC 30111:2019,信息技术 安全技术 漏洞处理
流程

[22] ISO 31000:2018,风险管理 指南

[23] 开放式 Web 应用程序安全项目 (OWASP),OWASP Web 安全测试指南,[在线][查看于 2020 年 12 月 3 日]。可在https://owasp.org/www-project-web-security获取
-测试指南/

[24] 开放式 Web 应用程序安全项目 (OWASP),OWASP Top 10,[在线] [2022 年查看 - 10-29]。可在https://owasp.org/Top10/获取

ICS 35.030
价格基于28页