



中华人民共和国国家标准

GB/T 32914—2023

代替 GB/T 32914—2016



信息安全技术 网络安全服务能力要求

Information security technology—Capability requirements of cybersecurity service

2023-09-07 发布

2024-04-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总体要求 2

5 一般要求 2

 5.1 基本条件 2

 5.2 组织管理 3

 5.3 项目管理 3

 5.4 供应链管理 5

 5.5 技术能力 5

 5.6 服务工具 5

 5.7 远程服务 6

 5.8 法律保障 6

 5.9 数据安全保护 6

 5.10 服务可持续性 7

 5.11 检测评估服务专项要求 7

 5.12 安全运维服务专项要求 7

6 增强要求 8

 6.1 基本条件 8

 6.2 组织管理 8

 6.3 供应链管理 8

 6.4 技术能力 8

 6.5 服务工具 8

 6.6 数据安全保护 9

 6.7 服务可持续性 9

 6.8 安全运维服务专项要求 9

附录 A（资料性） 网络安全服务使用的常见工具类型 10

参考文献 12

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 32914—2016《信息安全技术 信息安全服务提供方管理要求》，与 GB/T 32914—2016 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 将术语“信息安全服务”更改为“网络安全服务”，并更改了定义（见 3.1，2016 年版的 3.1）；
- b) 增加了总体要求（见第 4 章）；
- c) 将第 5 章、第 6 章内容更改并合并为“第 5 章 一般要求”（见第 5 章，2016 年版的第 5 章、第 6 章）；
- d) 增加了“供应链管理”要求（见 5.4）；
- e) 增加了“远程服务”要求（见 5.7）；
- f) 增加了“法律保障”要求（见 5.8）；
- g) 增加了“数据安全保护”要求（见 5.9）；
- h) 增加了“服务可持续性”要求（见 5.10）；
- i) 增加了“检测评估服务专项要求”内容（见 5.11）；
- j) 增加了“安全运维服务专项要求”内容（见 5.12）；
- k) 增加了“增强要求”内容（见第 6 章）；
- l) 增加了“网络安全服务使用的常见工具类型”内容（见附录 A）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国电子技术标准化研究院、中国网络安全审查技术与认证中心、中国信息安全测评中心、国家信息技术安全研究中心、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、公安部第一研究所、公安部第三研究所、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、工业和信息化部电子第五研究所、中国信息通信研究院、国家工业信息安全发展研究中心、杭州安恒信息技术股份有限公司、北京安信天行科技有限公司、北京神州绿盟科技有限公司、全知科技（杭州）有限责任公司、广州竞远安全技术股份有限公司、中国移动通信集团有限公司、北京市政务信息安全保障中心（北京信息安全测评中心）、奇安信科技集团股份有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、北京时代新威信息技术有限公司。

本文件主要起草人：杨建军、何延哲、李有元、程瑜琦、陆丽、史大为、霍珊珊、李秋香、陆臻、陈青民、朱雪峰、李彦峰、陈星、何刚、方兴、金达、王琰、张斌、徐克超、李智明、程潞样、韦国文、邱勤、李媛、宋宏涛、陈洪波、马力、白旭东、李伟旗、王连强、李豫然、陈广勇、张静、周顿科、张铁铮、俞政臣、刘健、路明、唐刚、王翔宇、万紫骞、鲁立、孟楠、戴方芳、于盟、赵冉、徐思嘉、吕泽伟。

本文件及其所代替文件的历次版本发布情况为：

——2016 年首次发布为 GB/T 32914—2016；

——本次为第一次修订。

信息安全技术 网络安全服务能力要求

1 范围

本文件规定了网络安全服务的能力要求,包括一般要求和增强要求。

本文件适用于指导网络安全服务机构开展网络安全服务,以及评价网络安全服务机构的能力水平,也可为网络安全服务需求方选择网络安全服务机构时提供参考。

注:本文件所述网络安全服务不含涉及国家秘密的网络安全服务。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GB/T 20984 信息安全技术 信息安全风险评估方法
- GB/T 22080 信息技术 安全技术 信息安全管理体系 要求
- GB/T 25069 信息安全技术 术语
- GB/T 36959 信息安全技术 网络安全等级保护测评机构能力要求和评估规范
- GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
- GB/T 42446 信息安全技术 网络安全从业人员能力基本要求
- GB/T 42461 信息安全技术 网络安全服务成本度量指南

国家网络安全事件应急预案(2017年1月10日 中央网络安全和信息化领导小组办公室〔2017〕4号公布)

网络产品安全漏洞管理规定(2021年7月12日 工业和信息化部 国家互联网信息办公室 公安部〔2021〕66号公布)

网络关键设备和网络安全专用产品目录(第一批)(2017年6月1日 国家互联网信息办公室 工业和信息化部 公安部 国家认证认可监督管理委员会〔2017〕01号公布)

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

网络安全服务 cybersecurity service

根据服务协议,基于服务人员、技术、工具、管理和资金等资源,提供保障网络运行安全、网络信息安全等服务的相关过程。

注1:常见的网络安全服务包括检测评估、安全运维和安全咨询等。

注2:网络安全服务通常以供需双方的服务项目形式进行。

注3:网络安全等级保护测评、商用密码应用安全性评估属于检测评估服务中的特定类别服务。

3.2

网络安全服务机构 cybersecurity service provider

提供网络安全服务(3.1)的组织。

注：简称“服务机构”。

3.3

网络安全服务需求方 cybersecurity service acquirer

获取外部所提供的网络安全服务(3.1),以满足网络安全需求,实现自身业务目标的组织或个人。

注：简称“服务需求方”。

3.4

服务协议 service contract

服务开始前供需双方共同签署,并在服务过程中共同遵守的约定。

注：服务协议形式上是服务合同及其附属的工作说明书。

3.5

服务水平 service level

在服务协议(3.4)中对服务交付成果明确约定、可测量和文档化的一系列服务指标。

3.6

服务要素 service factors

规划和实施服务所需的服务人员、服务流程、服务环境、服务方法、服务工具和服务保障等要素。

3.7

服务方案 service plans

基于服务目标,对服务各阶段中所需执行的过程、任务、活动以及相关服务要素(3.6)、服务水平(3.5)进行详细描述文档。

3.8

服务变更 service change

对服务范围、服务目标、服务依据、服务内容、服务水平(3.5)、服务价格和服务要素(3.6)等进行新增、修改或解除的活动。

4 总体要求

4.1 网络安全服务机构向网络安全服务需求方提供网络安全服务,应满足第5章的要求。网络安全服务机构向对网络安全服务有更高要求的服务需求方(如党政机关、关键信息基础设施运营者等)提供网络安全服务时,还应满足第6章的要求。

4.2 网络安全等级保护测评机构的要求应符合 GB/T 36959 的规定。

4.3 商用密码应用安全性评估机构的要求应符合国家密码管理有关法律法规和标准规范的规定。

5 一般要求

5.1 基本条件

服务机构应具备以下基本条件：

- a) 在中华人民共和国境内注册；
- b) 法定代表人、董事、合伙人以及高层管理人员三年内无犯罪记录；

注：以公司为例，高层管理人员包括总经理、副总经理、财务总监、技术总监和安全总监等。

- c) 未被列入可能影响网络安全服务的负面清单，如失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单和不可靠实体清单等；
- d) 不存在未处理的网络安全相关行政处罚和正在接受网络安全审查等情形。

5.2 组织管理

服务机构的组织管理应满足以下要求：

- a) 按照 GB/T 22080 建立信息安全管理体系统；
- b) 设置与网络安全服务规模相适应的专业技术部门或团队；
- c) 网络安全服务项目负责人具备 2 年以上相应网络安全服务项目经验；
- d) 建立服务人员档案，包括服务人员的资格证明、培训/考核记录、技术方向和能力水平、从业经历、实际参与项目及分工等信息，档案至少保存至服务人员离职后 6 年；
- e) 服务人员具备 GB/T 42446 规定的网络安全服务相关的知识和技能要求，熟练掌握《国家网络安全事件应急预案》《网络产品安全漏洞管理规定》等的要求，接受岗前培训并经考核评定合格后上岗；

注：岗位涉及使用网络安全服务工具（以下简称“服务工具”）的，培训及考核内容需涵盖服务工具实操部分；服务工具包括设备、平台、软件、模板和知识库等，常见服务工具类型见附录 A。

- f) 与服务人员签订保密协议，约定服务项目实施中的通用保密要求，并定期进行保密教育。

5.3 项目管理

5.3.1 服务成本度量

服务机构应按照 GB/T 42461 对网络安全服务项目的成本进行度量后合理确定服务报价。

5.3.2 服务方案

服务机构的网络安全服务方案应满足以下要求：

- a) 在服务项目实施前编制网络安全服务方案，并得到服务需求方的认可；
- b) 在服务方案中明确网络安全服务范围、服务目标、服务依据、服务内容及服务水平；
- c) 在服务方案中明确服务人员（包括项目负责人和项目实施人员的职责等）、服务流程（包括计划或进度等）、服务环境、服务方法、服务工具以及服务保障（包括资源保障、质量管理、保密管理和风险控制等）等服务要素。

注 1：涉及项目实施人员及职责的，具体到个人身份，并提供联系方式。

注 2：涉及服务流程中计划或进度的，至少具体到月份。

注 3：服务方法通常包括：人员访谈、资料查看、配置检查、漏洞扫描、渗透测试、源码分析、日志分析和系统监测等。

5.3.3 服务实施

服务机构在服务实施过程中的要求包括以下内容。

- a) 应根据服务方案组织项目实施，与服务需求方保持沟通、反馈，如采取通知、定期例会或报告等形式。
- b) 应建立服务变更管理流程，变更前与服务需求方就具体事项主动沟通，经服务需求方同意后，确保服务变更以受控的方式得到评估、批准和实施；服务变更后对服务目标、服务水平、服务需求方系统和业务造成影响的，应进行针对性的改进、补救或恢复。
- c) 应建立项目应急处置机制，确定双方的接口人，及时处理服务实施过程中产生的投诉、争议和突发事件等，并形成处置结论或解决方案。
- d) 在服务过程中发现网络安全事件，应及时向服务需求方报告安全事件情况，并根据国家网络安

全事件报告的有关规定报告安全事件。如网络安全服务涉及网络安全事件处置,应协助服务需求方根据《国家网络安全事件应急预案》及相关规定处置,并在服务需求方的服务器和终端等存储媒介妥善留存事件处置记录(包括事件原因、事件经过、事件影响、处置人员和处置结果等)和相关原始数据(如行为日志、网络数据包和有害程序样本等)。

- e) 在服务过程中发现网络产品(含硬件和软件)的网络安全漏洞时,应及时向服务需求方报告。涉及通用产品、其上游产品或者组件的,应根据《网络产品安全漏洞管理规定》进行报告。

注:通用产品是指已公开销售或开放授权,且被广泛应用的产品。

- f) 应对服务过程中的关键活动进行记录,包括但不限于:

- 1) 服务变更记录;
- 2) 接收数据和资料的记录;
- 3) 引入的供应商产品(包括名称、标识和版本)以及服务人员(名单);
- 4) 与关键人员沟通和访谈的记录;
- 5) 关键安全策略变更记录;
- 6) 进行补丁更新和系统加固的记录;
- 7) 与漏洞和安全事件处置有关的记录。

- g) 建立、维护服务档案(包括服务方案和服务记录等),且档案至少保存 6 年,有关法律法规和行业管理另有规定的除外。

- h) 不应转包网络安全服务。分包网络安全服务时,确保服务需求方事前书面同意,分包的服务内容应通过服务协议将网络安全服务的目标、责任和要求有效传递到涉及的供应商,并对其履约情况进行监督。

5.3.4 风险控制

服务机构在服务过程中的风险控制应满足以下要求:

- a) 识别服务要素产生的风险,提出应对措施并确认其有效性;
- b) 服务过程中的操作可能对服务需求方系统的功能和性能,数据的保密性、完整性、可用性和真实性等造成影响的,需向服务需求方进行风险提示,经服务需求方同意并采取风险规避措施(如在测试环境中仿真验证、进行系统和数据备份等)后方能实施;
- c) 采取必要的监督机制或审计措施,确保服务人员对系统和数据的操作不超出服务协议及服务需求方授权的范围;
- d) 对于可能影响网络安全服务质量的重大事项,如项目负责人及关键服务人员变更、服务机构业务转型、合并重组和投资并购等,提前向服务需求方报告。

5.3.5 成果交付

服务机构交付服务成果应满足以下要求:

- a) 按服务协议中所规定的关键节点,提交服务交付成果,如服务方案、服务过程文档和记录、服务报告(包括阶段报告、总结报告和验收报告等),并得到服务需求方的确认;
- b) 保证所有服务交付成果的真实性、准确性和完整性,能清晰阐明其中的依据、组成、结论、措施、数据来源及支撑材料等内容;
- c) 完成服务交付后,根据与服务需求方的约定,主动将服务需求方提供的数据、资料、访问凭证,开通的账号和部署的工具等进行交还、清理或卸载,并向服务需求方提供由项目服务人员签字的承诺或确认函。

5.4 供应链管理

服务机构的供应链管理应满足以下要求：

- a) 建立统一的采购和供应链管理制度,对供应商的基本条件、供应过程、供应变更等进行审核、监督和管理,基本条件满足 5.1c) 和 d) 中的条件;
- b) 对长期使用、依赖度高的产品和服务建立合格供应商目录,且同类产品和服务有多个合格供应商;
- c) 要求供应商声明不非法获取服务需求方数据、控制和操纵服务需求方系统和设备,或利用服务需求方对产品的依赖性谋取不正当利益或者迫使更新换代;

注: 声明的方式包括在合同内容中体现、签署专门的承诺书等。

- d) 在服务过程中需要引入供应商人员的,按照 5.2 对相关人员进行筛选、考核和管理;
- e) 在获知供应链相关的安全事件信息或威胁信息后,采取更新、中止或替换供应商等针对性的应急措施;
- f) 建立和维护供应过程档案,记录所有供应商 6 年内提供产品的名称、标识、版本、产地和生产商,服务的名称、涉及的人员名单及其简历等信息。

5.5 技术能力

服务机构的技术能力要求包括以下内容。

- a) 应对已开展的网络安全服务形成技术指导文档(包括技术规范、操作指引和用例集等),编制技术指导文档应重点关注以下内容:
 - 1) 网络安全服务相关法律法规、标准等中的要求、最佳实践等内容;
 - 2) 国内外权威机构发布的安全态势报告、漏洞公告、突发安全事件报告等中的最新安全威胁分析方法、脆弱性识别方法、安全加固指引等内容;
 - 3) 国内外网络安全技术等的发展动向中关于安全控制、技术解决方案等内容。
- b) 服务内容涉及网络安全事件处置的,应根据《国家网络安全事件应急预案》及相关国家标准要求,建立网络安全事件处置所需的技术能力,如编制相关工作程序、开展知识技能培训和进行实操演练等。
- c) 开展网络安全服务过程中,涉及使用密码的,应符合国家密码管理有关规定和相关标准规范要求。

5.6 服务工具

服务机构在服务过程中使用服务工具的要求包括以下内容:

- a) 服务工具被有关部门通报或从其他渠道获知(如行业曝光等)存在安全问题的,应立即停止使用直至问题被修复;

注: 经确认工具的版本不属于涉及安全问题的版本,或经证明问题不存在的除外。

- b) 服务工具为《网络关键设备和网络安全专用产品目录(第一批)》中的,应已通过国家检测认证;
- c) 应确保服务工具的合法版权且授权在有效期内,运行状态良好,并持续更新和升级;涉及模板和知识库的,应根据相关法律法规、标准及时更新;
- d) 应明确服务工具的使用方法,对工具使用人员进行培训,避免因不当操作对服务需求方系统、业务和数据造成影响;
- e) 应根据服务项目对服务工具使用权限进行分离,防止非授权服务人员使用服务工具的功能、访问工具中的日志和报告等数据;

- f) 应定期检验服务工具的安全性,如对工具进行杀毒、对工具产生的网络流量进行分析等,避免工具存在影响安全性的组件或功能,如隐蔽的链接、协议或端口等;
- g) 应关注服务工具及其组件的安全漏洞公告和相关信息,在发现漏洞被披露时,应第一时间评估漏洞的影响,在不影响服务需求方系统和业务等的前提下,采取更新补丁或下线工具等措施;
- h) 应确保使用服务工具的过程不会对服务需求方系统边界安全措施造成影响(如服务需求方系统被服务工具以外的其他非授权工具、终端或第三方系统绕过边界防护措施直接访问)。

5.7 远程服务

服务机构需要远程提供服务的(如远程操作服务工具和登录服务需求方系统等),应在服务需求方和服务机构双方约定下满足以下要求:

- a) 对远程登录操作人员进行实名登记,分配仅能自用的账号;
- b) 对远程登录操作人员进行身份鉴别,为账号设置复杂度高(如长度不少于12位,包含大写字母、小写字母、数字和特殊字符等三种以上的字符类型)的口令并定期更换;
- c) 远程登录操作仅限于指定的终端及客户端(如有),并对权限范围和时间周期进行限制;
- d) 远程登录操作时,采用密码技术建立安全的信息传输通道,保证通信过程中数据的保密性和完整性;
- e) 至少留存6个月内远程操作的日志,定期对日志进行审计,审计过程中发现存在网络安全事件的按照5.3.3d)的规定处置。

5.8 法律保障

服务机构的法律保障要求包括以下内容。

- a) 应由专业法务人员审核网络安全服务协议。
- b) 应在服务协议中明确以下内容:
 - 1) 服务机构与服务需求方双方的责任边界;
 - 2) 网络安全服务的范围、内容、目标、节点、水平、交付成果和验收等条款;
 - 3) 网络安全服务的数据安全保护、项目成果知识产权归属和保密承诺等条款;

注:数据安全保护条款具体见5.9a)。

- 4) 体现因需遵循的法律法规、政策变化影响而造成服务中断、停止服务或退出市场等的相关条款及相应责任。

5.9 数据安全保护

服务机构对服务过程中获取的数据(包括原始数据和加工分析产生的数据等)进行安全保护的要求包括以下内容。

- a) 在服务实施前,应与服务需求方明确约定数据安全保护的相关条款,包括服务过程中涉及的个人信息(如身份信息等)、业务数据、系统数据、安全数据及其他相关资料的保护要求,以及数据的使用目的和周期、最小处理范围、最小特权访问和事后处置等保护措施。

注1:约定数据安全保护的条款的方式包括在服务协议中专门体现或签署单独的数据安全保护协议。

注2:现场提供网络安全服务的,明确项目相关资料是否能被外带的要求。

注3:涉及纸质资料的,明确是否可被电子化。

- b) 不应将网络安全服务过程中获取的数据变更目的使用,不应向第三方提供或进行公开,服务协议中明确授权或经服务需求方同意的除外。
- c) 应采取必要的安全措施,如加密、签名和备份等,保证所获取数据的保密性、完整性、可用性和

真实性,未经服务需求方同意,不应更改、删除和销毁原始数据。

- d) 因服务所需向境外提供和传输网络安全服务过程中获取的各类数据,应在事前向服务需求方单独告知出境目的、数据种类、数量、周期和接收方等情况,取得服务需求方书面同意。同时,还应遵守数据出境管理相关法律法规的要求。
- e) 在服务实施完成之后,应按服务需求方和服务协议的要求,进行数据的脱敏、移交、清理或销毁等处理。服务需求方对处理情况提出核验或审计的,应予以充分配合。

注 4: 包括服务工具中残留数据的处置。

5.10 服务可持续性

服务机构保障服务可持续性的要求包括以下内容:

- a) 服务终止后,可能对服务需求方系统、业务和数据等造成影响的,应在服务期限到期前向服务需求方告知;
- b) 涉及服务机构更换的,应根据服务需求方要求向指定的其他服务机构移交相关的资料、账号、证件和令牌等;
- c) 如确有无法提供持续服务的情况,应提前向服务需求方告知相关情况,并提出服务需求方认可的替代或交接方案,以保障服务需求方业务的持续性。

5.11 检测评估服务专项要求

服务机构提供检测评估服务的专项要求包括以下内容:

- a) 服务机构应具备基本的检测评估相关服务工具研发能力或二次开发能力;

注: 利用脚本语言编写测试代码等认为是基本研发能力的体现。

- b) 服务内容涉及风险评估的,应按照 GB/T 20984 的规定对风险进行识别、定性或定量分析和评价;
- c) 开展漏洞扫描和渗透测试等可能会对服务需求方系统、业务和数据等造成影响的,应向服务需求方单独告知影响、风险及应对措施,经服务需求方同意后采取影响最小的方式实施;
- d) 服务需求方要求使用测试环境进行检测评估时,应分析测试环境与真实环境(如生产环境)的区别,向服务需求方告知检测评估结果的适用范围;
- e) 应针对检测评估所发现的安全问题和风险等提出安全整改建议,并在服务需求方完成整改后验证整改效果,服务需求方无相关需求的除外;
- f) 检测评估报告等服务交付成果应至少保存 6 年,有关法律法规和行业管理另有规定的除外。

5.12 安全运维服务专项要求

服务机构提供安全运维服务的专项要求包括以下内容:

- a) 维持安全运维服务团队的稳定性,驻场服务人员每年或单个项目服务期间更换比例原则上应不超过 30%;

注 1: 如更换比例超过 30%,向服务需求方告知更换服务人员的原因,以及采取何种保障措施确保服务水平不会下降。

- b) 安全运维服务团队应具备对网络攻击行为进行主动发现、分析和提出防护建议的能力;

注 2: 发现方式包括日志分析、异常文件分析、异常进程分析、异常流量分析和威胁源分析等。

- c) 对运维工作记录进行汇总,定期向服务需求方提供安全运维工作简报,简报的形式和提交时间应在服务协议或服务方案中明确,包括日报、周报、月报、季报和年报等形式;
- d) 应通过运维事件响应和事件关闭率等可量化的指标,衡量安全运维的服务水平和用户满意度;

- e) 服务交付成果中应包含服务周期内的安全运维总结报告,总结报告内容包括安全运维工作的基本情况、处置的安全事件、采取的改进措施和服务水平评价数据等。

6 增强要求

6.1 基本条件

服务机构应具备以下条件:

- a) 法定代表人、董事、合伙人以及高层管理人员无犯罪记录;
- b) 2年内没有因重大网络安全服务问题被有关部门通报。

6.2 组织管理

服务机构组织管理应满足以下要求:

- a) 指定一名高层管理人员作为网络安全服务负责人;
- b) 根据服务协议中的服务内容建立相对独立的项目服务团队(服务期内保证不少于50%服务人员仅服务特定项目);
- c) 对项目服务人员进行背景审查,审查结果长期留存并可供服务需求方查看;项目服务人员的身份和安全背景等发生变化(如取得非中国国籍)或必要时,重新进行背景审查;
- d) 确保项目服务人员是持有相关技术资格证明且任职1年以上的员工,且无信息网络犯罪记录;
- e) 确保项目服务人员每人每年教育培训时长不少于30个学时,教育培训和考核内容包括网络安全相关法律法规、政策标准、网络安全保护技术、管理知识和实操技能等;

注:常见的实操技能包括网络攻击演练或沙盘推演、威胁及入侵痕迹分析、攻击阻断和安全加固和网络安全事件处置等。

- f) 确保项目服务人员已掌握保密相关知识和技能(如通过保密培训及考试),知晓了其应当履行的安全保密义务和承担的法律 responsibility,包括安全职责、保密内容、奖惩机制和保密期限等,并分别与服务需求方签署保密协议(或承诺书和责任书)。

6.3 供应链管理

服务机构在服务过程中需要引入供应商产品或服务的,应对政治、贸易和外交等因素导致产品或服务供应中断的风险进行评估,优先选择合格供应商目录中供应有保障的产品或服务。

注:如选用具有自主知识产权、有备份方案的产品或服务。

6.4 技术能力

服务机构的技术能力要求包括以下内容:

- a) 应按照 GB/T 39204—2022 中第9章的相关内容,通过建立与国家、行业等有关管理部门、研究机构、其他网络安全服务机构、服务需求方和业界专家的合作机制,共享网络安全信息;

注:网络安全信息包括但不限于漏洞信息、威胁信息、最佳实践和前沿技术等。

- b) 应建立网络安全服务管理系统,将网络安全服务的基本情况和 5.3.3 d)~f) 涉及的记录录入系统并进行自动化管理,且系统可支持通过接口方式共享相关记录。

6.5 服务工具

服务机构在服务过程中使用服务工具的要求包括以下内容:

- a) 应针对服务项目建立单独的服务工具清单,并明确服务工具的使用要求和范围;

- b) 服务工具需接入服务需求方生产环境的,应取得安全认证或通过第三方机构的安全检测;
- c) 服务工具无法使用会对服务水平产生显著影响的,应通过提前采购储备、同类型产品备份或签署备货协议等方式保障服务工具的持续供应。

6.6 数据安全保护

服务机构对服务过程中获取的数据进行安全保护的要求包括:

- a) 服务过程中应对网络安全服务产生的网络流量数据进行监测或审计,保证所有网络流量数据均为提供服务所必需;涉及出境流量数据的,应按照 5.9d) 的规定处置;
- b) 服务过程中获取的数据,应与其他数据分开存储和处理,并按照 GB/T 39204—2022 中 7.10 的规定予以保护;
- c) 对服务过程中获取的原始数据进行加工、分析和使用(如数据脱敏后的态势分析和算法训练等)应经服务需求方同意,并满足相关法律法规和行业管理规定的要求。

6.7 服务可持续性



涉及服务机构更换的,服务机构应确保网络安全服务工作顺利交接后才可退出服务。

6.8 安全运维服务专项要求

服务机构提供安全运维服务的专项要求包括以下内容:

- a) 应保证运维地点位于中国境内,如确需境外运维,应符合法律法规要求及相关规定;
- b) 安全运维服务团队应具备对服务需求方暴露面进行识别的能力;

注:识别内容包括:互联网和内网资产的互联网协议地址、端口和应用服务,互联网上的内部信息(组织架构、邮箱账号和组织通讯录等),公共存储空间(如,代码托管平台、文库和网盘等)的可能被攻击者利用的技术文档等。

- c) 安全运维服务团队应具备对不同厂商安全设备产生的日志进行整合分析,以及对 5.3.3f) 中记录的、服务需求方所掌握的以及从其他渠道获知的网络安全信息进行汇总和研判的能力。

附 录 A

(资料性)

网络安全服务使用的常见工具类型

A.1 漏洞扫描工具

通过远程或现场的方式,对网络安全隐患进行探测、检查和分析,发现目标系统在设计、实现、配置和运行等过程中,有意或无意产生的脆弱性或后门,并提出一定的防范和补救措施建议的工具。

A.2 漏洞挖掘工具

针对目标系统,通过代码审核、模糊测试和静态分析技术等多种方法,经综合分析,发现目标系统在设计、实现、配置和运行等过程中,可能存在的脆弱性或后门,并提出一定的防范和补救措施建议的工具。

A.3 配置核查工具

基于安全配置要求实现对资产(如服务器、网络设备、安全产品、操作系统、数据库和应用系统等)的安全配置检测和合规性分析,生成安全配置建议和合规性报告的工具。

A.4 软件成分分析工具

通过分析软件包含的一些信息和特征,基于人工智能(AI)的分析引擎发现软件及其第三方组件的构成情况、引用位置和漏洞信息等,实现对软件的识别、管理、追踪的工具。

A.5 应用安全检测工具

通过代理、虚拟专用网络(VPN)或在服务端部署客户端程序,收集、监控应用程序(如 Web 应用)运行时函数执行和数据传输,并与扫描器端进行实时交互,高效、准确地识别应用层面的安全缺陷及漏洞,确定漏洞所在的代码文件、行数、函数及参数的工具。

A.6 源代码审计工具

从源代码层面对应用系统进行安全审计和分析,发现源代码中可能存在的安全缺陷或隐患,识别安全漏洞,检测编码规范性的工具。

A.7 流量分析工具

针对网络或者被测试系统的交互流量能够捕获、截断、重放和修改的分析工具。

A.8 风险评估与管理工具

支撑风险评估全过程的高效实施和自动化管理的工具,包括被评估信息系统基本信息获取、资产信息获取、脆弱性识别与管理、威胁识别、风险计算、评估过程与评估结果管理、提出风险控制措施等功能。

A.9 安全审计工具

用于记录系统、设备、应用程序、终端和个人等产生的网络日志,分析网络安全现状,协助审计及合规管理等人员进行尽责调查和合规性检查的工具。

A.10 资产发现工具

通过接入被评估网络,对网络地址和可访问网络链接进行探测,识别并标注网络资产的相关信息(包括存活情况、服务、端口和操作系统等)的工具。

A.11 资产信息收集工具

通过提供调查表形式,收集被评估信息系统数据、管理和人员等资产信息,调研组织的主要业务、重要资产、威胁、管理上的缺陷、采用的控制措施和安全策略的执行情况的工具。

A.12 入侵检测/防御系统



通过部署检测引擎,收集和处理整个网络中的通信信息,分析其是否构成对网络或主机造成危害的入侵攻击事件,生成相应的告警信息且必要时进行主动防御的系统。

A.13 应急响应辅助系统

为应急响应提供辅助,对安全事件进行影响分析、生成处置计划和向相关人员分配工作任务等,实现应急响应部分工作的自动化支持的系统。

参 考 文 献

[1]	GB/T 30271—2013	信息安全技术	信息安全服务能力评估准则
[2]	GB/T 30276—2020	信息安全技术	网络安全漏洞管理规范
[3]	GB/T 31168—2014	信息安全技术	云计算服务安全能力要求
[4]	GB/T 34942—2017	信息安全技术	云计算服务安全能力评估方法
[5]	GB/T 36626—2018	信息安全技术	信息系统安全运维管理指南
[6]	GB/T 36637—2018	信息安全技术	ICT 供应链安全风险管理体系指南
[7]	GB/T 36643—2018	信息安全技术	网络安全威胁信息格式规范
[8]	GB/T 38645—2020	信息安全技术	网络安全事件应急演练指南

