ICS 33.050
CCS M 30

团　体　标　准

T/TAF 182—2023

网络产品应急响应安全要求　技术要求

Security requirements for network product emergency response—Technical requirements

2023-09-11 发布　　2023-09-11 实施

电信终端产业协会　发布

目　　次

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。

本文件中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、上海泰峰检测认证有限公司、博鼎实华（北京）技术有限公司。

本文件主要起草人：吴荣春、刘欣东、罗丹、张亚薇、薄菁、宋祥烈、刘向东。

引　　言

随着各行业、领域信息化工作的深入开展，越来越多承载信息系统的网络产品进入了运行维护阶段。然而，提供运行维护服务的各类组织的能力水平参差不齐，需方缺乏评价方法、手段及规范。而且网络产品作为支持信息化领域建设的重要组成部分，需要制定针对网络产品的应急响应安全技术要求，当网络产品发生事故时，能够在最短时间启动应急响应机制。本文件主要在网络产品在应急响应管理生命周期中提出应急事件监测分析、应急响应技术保障、应急事件响应等安全技术要求。

网络产品应急响应安全要求　技术要求

1　范围

本文件规定了网络产品在实际运行维护阶段应满足的应急响应安全技术要求，主要从应急事件监测分析、应急响应技术保障、应急事件响应等方面提出针对使用网络产品的实际运行维护方的安全技术要求。

本文件适用于指导网络产品的使用方建立和维护网络产品应急响应技术体系，也可为第三方机构开展测评时提供参考。

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 28827.3　信息技术服务运行维护　第3部分：应急响应规范

GB/T 32914　信息安全技术　网络安全服务能力要求

GB/T 39276-2020　信息安全技术　网络产品和服务安全通用要求

GB 40050-2021　网络关键设备安全通用要求

GB 42250-2022　信息安全技术　网络安全专用产品安全技术要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

网络产品　network product

作为网络组成部分以及实现网络功能的硬件、软件或系统，按照一定的规则和程序实现信息的收集、存储、传输、交换和处理。

[来源：GB/T 39276-2020,3.2]

3.2

应急事件　emergency event

导致或即将导致运行维护服务对象运行中断、运行质量降低，以及需要实施重点时段保障的事件。

[来源：GB/T 28827.3-2012,3.2]

3.3

应急响应　emergency response

组织为预防、监控、处置和管理应急事件所采取的措施和活动。

[来源：GB/T 28827.3-2012,3.3]

3.4

风险评估 risk assessment

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。
[来源：GB/T 28827.3-2012,3.2]

4 缩略语

下列缩略语适用于本文件。
ISP：网络业务提供商（Internet Service Provider）
IPS：入侵防御系统（Intrusion Prevention System）
IDS：入侵检测系统（Intrusion Detection System）

5 技术支撑框架

在执行网络产品应急响应安全管理过程中，本文提出了一种技术框架（如图 1 所示），主要包含应急事件监测分析、应急响应技术保障、应急事件响应等安全技术要求。

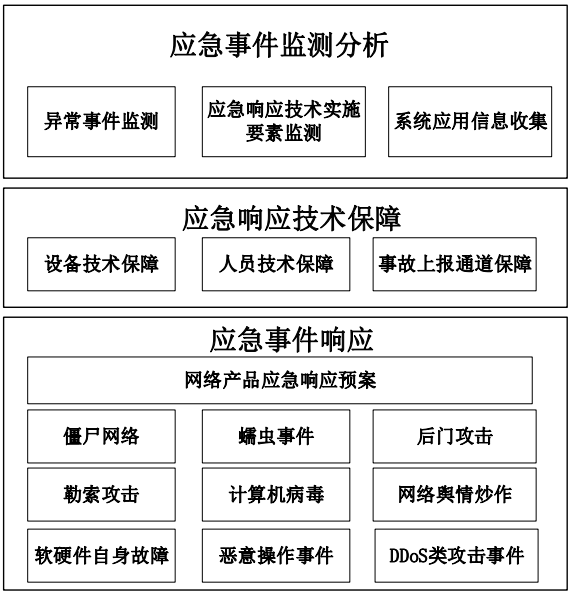

图 1 网络产品应急响应安全技术框架

6 应急事件监测分析

6.1 异常事件监测

网络产品使用方应储备支持监测可疑网络流量、业务服务器是否崩溃、访问业务健康状态、信息系统日志中的可疑配置更改操作、多次失败登录、未经授权的对外网络连接、违反访问业务安全策略的事件、感染蠕虫、病毒、恶意软件等以下监测分析技术以能够实时监测网络异常事件：

a) 应支持监测出可疑网络流量（如激增的拒绝服务类流量以及能够影响网络正常运行的流量）并产生告警；
b) 应支持监测业务服务器是否崩溃；
c) 应支持监测访问业务健康状态；
d) 应支持监测信息系统日志中的可疑配置更改操作；
e) 应支持监测针对网络关键设备或信息系统接入多次失败登录等异常操作；
f) 应支持监测未经授权的对外网络连接；
g) 应支持监测违反访问业务安全策略的事件；
h) 应支持监测利用已知漏洞攻击的事件，并发出告警；
i) 宜支持监测被感染蠕虫、病毒，或其他形式的恶意逻辑命令符，并发出告警；
j) 宜支持监测恶意软件，对被怀疑为恶意代码的软件组件进行分析告警，并确定事件的影响范围。

6.2 应急响应技术实施要素监测

应定期通过以下技术手段监测应急响应技术实施要素是否完备：

a) 开展风险评估中风险识别的脆弱点、风险点是否有缺失，规避风险的措施是否有效；
b) 在风险评估的基础上监测各种信息安全事件发生时对网络运行环境可能产生的影响是否全面；
c) 在业务中断、系统宕机、网络瘫痪等信息安全事件发生后应急响应策略以及处理的技术手段是否完善；
d) 应急响应所需设施、工具等是否齐全。

6.3 系统应用信息收集

应通过以下技术手段对系统应用的信息进行收集，收集的信息包括应收集易变的数据、收集持久数据、证据收集过程日志：

a) 应收集易变的数据，最大限度减少对信息系统的影响，审核易变数据可以了解网络系统的状态和当前正在运行的进程，通常包括各种日志、文件、配置设置、当前/过去登录用户记录、正在运行的进程、打开的文件、文件修改或系统设置（访问控制列表、注册表信息和权限）、捕捉的屏幕快照图像等，以此确定事件的日期、事件和起因；
b) 收集持久数据同时要防止网络系统的数据被覆盖。持久数据是指网络系统硬盘的数据和断电后不会改变的移动存储介质的数据，包括磁盘映像（文件、隐藏文件、删除数据、闲置空间、交换文件和未分配空间）、精确复制原始数据的过程；
c) 证据收集过程日志，包含在证据收集过程中所采取的一切行动的时间标记记录。记录的目的是使过程得到验证，并确保数字证书是对原始数据的精确标识。使用合理的取证方法和工具来

捕捉数据或证据，可以避免或减少证据被污染的情况。获取、保存、分析信息系统历史文件的过程可以帮助描述事件和策划下一步行动方案。

7 应急响应技术保障

7.1 设备的技术保障

网络产品中设备应至少满足GB/T 39276-2020中基本级安全要求，涉及网络关键设备应满足GB 40050-2021要求，涉及网络安全专用产品的应满足GB 42250-2022要求。

7.2 人员的技术保障

提供网络安全服务应急响应工作的人员应具有与所开展网络安全服务相适应的技术能力，并满足GB/T 32914中关于技术能力的要求。

7.3 事故上报通道保障

7.3.1 个人或用户的报告

应具备通过个人或用户上报应急事件的技术通道，当用户或管理员发现网络事件，报告相关信息到指定的事件收集联络点，可通过电话、电子信箱等方式上报，当指定事件收集联络部门收集到事件告警后，应按照应急事件类型快速制定应急预案。

7.3.2 其他内部或外部构成组织机构的事故报告

应支持通过其他内部或外部构成组织机构进行应急事件事故上报的技术管理通道，可通过电话、电子信箱等方式上报，当指定事件收集联络部门收集到事故告警后，应按照应急事件类型快速制定应急预案。

8 应急事件响应

进入应急响应环节，按照初步研判的安全事件等级进行应急响应。

a) 当网络发生故障时，先判断破坏的来源与性质：
   1) 如果是自然灾害导致的，根据网络平台的实时监测，采取恢复措施；
   2) 如果是设备损坏导致的故障，断开影响安全和稳定的信息网络设备，断开与破坏来源的物理链接，平滑过渡到备份设备，修理或更换损坏的设备；
   3) 如果是人为破坏，定位损坏的设备，断开影响安全和稳定的信息网络设备，断开与破坏来源的物理链接，跟踪并锁定破坏来源的 IP 地址或其他网络用户信息，修复被破坏的信息，恢复网络。
b) 按照故障发生的不同情况分别采取以下措施：
   1) 网络攻击，当发现黑客正在进行攻击时或者已经被攻击时，可采用关闭接口的方式将被攻击的路由器、交换机等设备从网络中隔离出来，并将有关情况记录并向上级汇报；应急实施人员在接到通知后立即赶往现场，对现场进行分析，并做好记录；对该设备的配置进行数据备份；恢复与重建被攻击或破坏的系统。
   2) 广域网外部线路中断紧急处置措施，广域网线路中断后，应急日常运行小组人员应立即向负责人报告；负责人员接到报告后，应迅速判断故障节点，查明故障原因并记录；如属于

内部职责，应立即予以恢复；如属于 ISP 部门管辖范围，应立即与 ISP 维护部门联系，要求修复；视故障严重性，如有必要，向上级部门主管书面汇报。

3) 局域网中断紧急处置措施，设备管理部门准备好网络备用设备，存放在指定的位置；局域网中断后，应急日常运行小组人员应立即研判故障节点，查明故障原因，并向应急实施小组成员汇报；如属于线路故障，应重新安装线路；如属于路由器、交换机等网络设备故障，应立即从指定地点将备用设备取出调试；如属于路由器、交换机配置文件破坏，应迅速按照要求重新配置或者启用备份文件，并调试通畅；如有必要，需逐级向上级领导书面汇报。

c) 按照事件发生的不同类型采取不同的应急响应技术措施，参考附录A网络产品应急响应技术预案。

附 录 A
（资料性）
网络产品应急响应技术支撑预案

A.1 僵尸网络事件应急预案

A.1.1 应急启动

在安全事件检测过程中，如发现局域网连接数增加、对系统资源占用导致服务器明显变慢或资源耗尽、网站服务器被远程安装异常软件和程序等情况，应根据判定依据对安全事件类型进行确认，主要包括以下四点：

a) 在命令行（如windows中cmd.exe）里输入“netstat -an”命令，如果出现本地 IP 向多个目标 IP的相同端口（如135、445等）发起连接的现象，则很可能是扫描行为；
b) IPS出现重复性地与外部的 IP 地址连接或非法的 DNS 地址连接日志；
c) IDS上出现大量的协议监测网络通信内容；
d) 防病毒软件上存在大量未查杀的病毒信息记录。经现场确认为僵尸网络事件时，启动本预案。

A.1.2 应急处置

僵尸网络事件应急预案启动后，应根据以下流程进行应急处置：

a) 关闭或断开问题服务器；
b) 查看防火墙策略、连接和端口流量，开启调试模式（如Debug）并配置防火墙策略阻断该问题IP；
c) 通过端口连接和异常的进程进行定位，查杀该进程；
d) 重新启动问题服务器，刷新服务器的连接池，恢复应用初始状态；
e) 通过持续关注服务器的连接数、访问WEB页面速度、安全设备相关告警信息等，确认网络状态是否恢复正常；
f) 如恢复则通过日志查找问题应用或进程，找到后卸载问题应用，关闭问题进程，修改注册表；如未恢复或未找到问题应用或进程，则重新安装问题服务器；
g) 使用补救工具，如防范恶意代码或防病毒产品可以检测并清除隐藏的rootkit感染；
h) 后续可利用蜜罐（Honeypot）部署多个蜜罐捕获传播中的僵尸程序（如Bot）记录该程序的网络行为（如网络流量重定向工具Honeywall）。通过人工分析网络日志并结合样本分析结果，可以掌握该程序的属性，包括它连接的服务器、端口、频道、控制口令等信息，获得该僵尸网络的基本信息甚至控制权。

A.2 蠕虫事件应急预案

A.2.1 应急启动

当网络安全事件发生，经现场确认为蠕虫事件时，启动本预案，判定方式如下：

a) 网络速度减慢，“DNS”和“IIS”服务遭到非法拒绝，用户不能正常浏览网页；

b) 网络被阻塞，不稳定甚至瘫痪，交换机资源被大量消耗，流量被大量占用，CPU、内存被大量占用；
c) 检查防病毒网关的日志，查看异常告警信息；
d) 检查IPS的日志，查看异常告警信息；
e) 检查出口及各个网络区域的IDS设备日志，查看异常告警信息；
f) 检查系统服务器文件是否被篡改、加密。

A.2.2 应急处置

蠕虫事件应急预案启动后，应根据以下流程进行应急处置：
a) 隔离中毒服务器，启用备用服务器或系统；
b) 根据病毒特征，使用专用工具进行查杀；
c) 重装中毒服务器，导入备份数据；
d) 利用部署的企业版杀毒软件对服务器进行清查；
e) 对涉事服务器同Vlan的服务器群进行相关蠕虫的查杀。

A.3 后门攻击事件应急预案

A.3.1 应急启动

当网络安全事件发生，经现场确认为后门攻击事件时，启动本预案。
a) 基于网页的后门攻击在安全事件检测过程中，如发现网站页面被替换或者信息被篡改、页面运行不正常、自动下载不明程序等情况，应根据判定依据对安全事件类型进行确认。主要包括以下三点：
   1) 服务器区安全设备 IPS 发现木马后门类检测的告警日志。
   2) 服务器区的安全设备 WAF 有大量攻击日志。
   3) 网站上有上传的不明文件，如在图片库中发现可执行文件等。
b) 基于系统的后门攻击在安全事件检测过程中，如发现植入的远程控制软件、恶意修改系统管理员口令或者 WEB 应用管理员口令、新增文件或丢失等情况，应根据判定依据对安全事件类型进行确认，主要包括以下五点：
   1) 系统账号无法登录/异常登录。
   2) 有新增的不明用户。
   3) 新增异常进程。
   4) 出现未知的端口连接行为。
   5) 新增系统文件或丢失。

A.3.2 应急处置

后门攻击事件应急预案启动后，应根据以下流程进行应急处置：
a) 基于网页的后门攻击
   1) 将问题页面/服务器进行隔离。
   2) 安装 Webshell 查杀工具、安全狗等相关功能软件，对网站上的后门进行及时的查杀。

3) 根据 WEB 日志和系统日志，人工排查可疑文件，查找后门程序，将发现的后门程序删除。
4) 通过防火墙封禁触发告警的源 IP 地址。
5) 针对页面利用备份文件进行网站恢复。
6) 加强网站安全监测，防范网页恶意篡改及信息泄露。

b) 基于系统的后门攻击
1) 将问题服务器进行隔离。
2) 通过终端防病毒软件、反 root kit 工具等进行恶意程序查找，并清除恶意程序。
3) 通过防火墙封禁触发告警的源 IP 地址。
4) 根据系统日志，人工排查可疑文件，注意系统运行状况及文件增减情况，查看是否有异常服务启动项运行，及时终止。
5) 使用第三方杀毒软件全天监控、定时扫描查杀，定时更新系统补丁。

A.4 勒索攻击事件应急预案

A.4.1 应急启动

勒索病毒最终以勒索钱财为目的，当遭受勒索病毒攻击后会产生极为明显的受勒索特征。当网络安全事件发生，经现场确认为勒索病毒攻击事件时，启动本预案，具体可通过以下三种方式来进行判断中毒类型是否为勒索病毒：

a) 桌面壁纸被篡改，为了让受害者第一时间感知到被病毒入侵，攻击者通过修改用户桌面壁纸的方式告知用户已被病毒感染，需要缴纳赎金。
b) 有明显的勒索信息窗口展示，勒索病毒加密文件完成后，通常会在被加密文件所在目录下创建一个勒索提示说明文档，勒索病毒加密文件完成后通常会自动打开该文档，通常以 TXT、HTML 或病毒程序弹出窗口的形式呈现。
c) 文件后缀被修改并且文件使用打开异常，勒索病毒通常为了标识文件被自身加密过，当对文件加密完成后，会修改被加密文件的原始后缀，被修改后的文件后缀区别于常见文件类型，通过该后缀可以判断是否遭受了勒索病毒攻击。

A.4.2 应急处置

勒索病毒攻击事件应急预案启动后，应根据以下流程进行应急处置：

a) 采用物理隔离或访问控制的方式隔离受感染的主机。物理隔离指对于受感染的主机，在局域网内进行断网处理，确认勒索病毒清理完毕且经评估无风险后才能重新接入网络。访问控制指的是采用在安全设备中增加策略、关闭不必要的端口、修改登录口令等方式对访问的网络资源的权限进行严格的认证和控制，避免勒索病毒横向传播导致局域网内其他主机被动染毒。
b) 检查局域网内其他主机、核心业务系统等是否受到影响，备份系统是否被加密等，确定感染范围，评估存在的风险。
c) 对勒索病毒进行杀毒处理，对勒索病毒的行为进行分析，了解攻击发生的事件、现象，寻找并清理病毒进程，删除相关注册表及文件。
d) 及时更新安全补丁，对系统进行升级处理，关闭不必要的端口。

A.5 计算机病毒事件应急预案

A.5.1 应急启动

在安全事件检测过程中，如发现正常网页无法打开、遭到篡改、服务器出现宕机、蓝屏等情况，应根据判定依据对安全事件类型进行确认，依据如下：

a) 网页所属服务器内的文件被删除或受到不同程度的损坏。
b) 服务器系统出现可疑登录信息。
c) 服务器系统出现新增的可疑用户。
d) 破坏引导扇区及BIOS，硬件环境破坏。
e) 检查防病毒网关的日志，查看异常告警信息。
f) 检查IPS的日志，查看异常告警信息。
g) 服务器内出现多个相同名称的进程。
h) 服务器系统文件出现非正常隐藏文件夹。
i) 注册表中出现可疑的注册项。

经现场确认为计算机病毒事件时，启动本预案。

A.5.2 应急处置

计算机病毒事件应急预案启动后，应根据以下流程进行应急处置：

a) 隔离中毒服务器，启用备用服务器或系统。
b) 根据病毒特征，使用专用工具进行查杀。
c) 重装中毒服务器，导入备份数据。
d) 通过部署的企业版杀毒软件对服务器进行清查。
e) 对涉事服务器同 Vlan 的服务群进行相关木马文件的排查和查杀。

A.6 网络舆情炒作事件应急预案

A.6.1 应急启动

在安全事件检测过程中，如因出现的热点舆论信息造成了负面影响，启动本预案，负面影响主要包括以下内容：

a) 发现恶意攻击、扭曲国家形象的言论、图片等。
b) 发现针对国家发布的政策、法规、条文等内容进行恶意解读、歪曲内容、引导错误言论的行为。
c) 发现涉及黄赌毒、非法组织、非法言论等违法违规的内容。

A.6.2 应急处置

网络舆情炒作事件应急预案启动后，应根据事件调查结果、事件的性质、重要程度及舆情发展的态势（由一般到严重），分别采取以下信息公开方式：

a) 关闭相关问题网页或网站，删除网络舆情炒作事件的相关内容。
b) 对涉事网站的信息平台进行冻结，关闭评论或回复功能。或者进行已造成严重后果的，关停网站，关闭上述平台的相关板块。

c） 必要时限制或关闭涉事信息平台的用户注册功能，并对相关敏感词汇进行过滤。

d） 通知平台管理人员对恶意敏感信息进行集中清理。对涉嫌煽动、鼓动行为的账号进行禁封。

e） 条件许可情况下，针对舆论热点所涉及的核心问题，在信息平台上及时发送通告，阐明事实，稳定舆论。

f） 对事件情节严重的、对社会造成严重影响、扰乱社会政策秩序的，应交由网安部门和司法机关处理。保留相关服务器原始数据，包括但不限于应用数据、服务器系统日志、应用日志等，以便网安部门和司法机关进行检查。

g） 事件发生后或处于重大敏感时期时，应安排相关人员进行 24 小时值守，并随时保持相关人员的通讯畅通，接到命令必须按时到达地点，应急日常运行小组人员要有健全的值班记录制度。加大监管力度，对有组织、有煽动性等网上行为的言论及时进行记录、通报和处理，避免事态扩大。

A.6.3 善后工作

网络舆情应急处置结束后，相关责任部门及人员应持续关注网络上相关事件的舆情趋势，判断事件出现的缘由，必要时利用官方网站、媒体等方式进行公开声明。

A.7 软硬件自身故障事件应急预案

A.7.1 应急启动

在安全事件检测过程中，如发现硬盘故障、应用系统崩溃、操作系统崩溃、关键网络连接设备（如路由器、交换机等）故障时，启动本预案。

A.7.2 应急处置

软硬件自身故障事件应急预案启动后，应根据设备类型、故障情况选择不同的措施，应急处置方式主要包括以下内容：

a） 非硬盘硬件故障（CPU、内存、主板、网络适配卡）

1） 更换损坏的硬件或直接更换主机（仍使用原来的硬盘）。

2） 修复或更新损坏的硬件作为新的备件。

b） 硬盘故障（RAID 有效－文件系统仍可以正常读取）

1） 取出受损硬盘。

2） 插入新的硬盘（相同容量和型号）并重建。

c） 硬盘故障（RAID无效）

1） 备份用户数据（包括工作文件、电子邮件等）。

2） 备份关键配置文件和系统文件。

3） 取出受损硬盘并插入新硬盘。

4） 重建 RAID 系统。

5） 使用紧急恢复盘重新引导系统。

6） 载入镜像文件（包含标准的操作系统、应用程序和其他必要工具软件）恢复装有系统的文件系统。

7） 恢复用户数据和系统配置。
8） 应用系统崩溃。
9） 备份应用系统用户数据、系统文件和配置文件。
10）重新安装应用系统和相应的补丁程序。
11）恢复系统配置。
12）恢复用户数据。

d） 操作系统崩溃（软件原因）
1） 关闭系统并使用紧急恢复盘重新引导系统。
2） 载入镜像文件（包含标准的操作系统、应用程序和其他必要工具软件）恢复装有系统的文件系统。
3） 恢复原有系统配置。

e） 关键网络连接设备（路由器、交换机等）故障（冗余设备失效）
1） 更换相同型号的备用设备。
2） 从备份恢复原先的系统配置。
3） 重建冗余设置。
4） 修复或替换损坏设备作为新的备用设备。

f） 防火墙硬件故障（冗余设备失效）
1） 更换相同型号的备用设备。
2） 从备份恢复原先的系统配置。
3） 重建冗余设置。
4） 修复或替换损坏设备作为新的备用设备。

g） 防火墙软件故障（冗余设备失效）
1） 使用安装盘重新初始化防火墙系统。
2） 从备份恢复原先的防火墙系统配置。
3） 重建冗余设置。

A.8 恶意操作事件应急预案

A.8.1 应急启动

当网络安全事件发生，经现场确认为恶意操作事件时，启动本预案，具体现象如下：

a） 人为破坏网络线路、通信设施：通信线路、网络节点设备及端口配置被人员蓄意破坏/修改，导致网络通信异常、各网络节点设备运行异常以及网络节点存在接口异常。

b） 系统服务器遭到破坏：应用服务被人员蓄意删除或禁用导致服务器上应用进程崩溃、无法提供相应的应用服务；人员蓄意损坏电源、硬盘、内存、处理器、主板等硬件设备导致服务器蓝屏、死机或无法正常开关机。

A.8.2 应急处置

恶意操作事件应急预案启动后，应根据以下流程进行应急处置：

a） 人为破坏网络线路、通信设施
1） 系统自动/手动切换到备用线路。

2) 检测通信网络故障位置。内部线路遭到破坏，保护现场，调取监控录像，查找问题人员，根据造成破坏的程度确定是内部处罚还是交给公安机关进行处置；外部线路遭到破坏，及时联系相关运营商，要求及时恢复线路通讯，并要求说明故障原因。

b) 系统服务器遭到破坏

1) 当发现服务器软件系统出现故障，首先启用备用服务器，保证业务的正常运行。

2) 其次确认服务器故障情况：服务器系统出现软件故障时，尝试登录服务器进行检查，如能登录服务器，对服务器系统杀毒，升级相关系统软件；若故障依然存在，使用备份系统进行还原，进入“目录服务还原模式”还原系统实时状态；如不能登录服务器，联系厂家进行维修。

3) 当服务器出现硬件故障，通过以下步骤排除：确定故障原因。依次查看电源、硬盘、内存、主板、处理器等，如条件许可，可使用替换法检测各硬件；恢复固件缺省配置，如去除第三方厂商配件和非标配部件；清除 CMOS，恢复资源初始配置。

A.9 DDoS 类攻击事件应急预案

A.9.1 应急启动

在安全事件检测过程中，如发现系统流量异常激增、应用进程拒绝服务、系统瘫痪、流量阈值告警等事件，启动本预案。

A.9.2 应急处置

DDoS 攻击事件应急预案启动后，应根据以下流程进行应急处置：

a) 隔离被攻击的服务器业务访问地址，启用备用服务器或系统业务地址。

b) 关停不必要的服务和端口，实现服务最小化，例如WWW服务器只开放80而将其他所有端口关闭或在防火墙上做阻止策略。

c) 如攻击的服务端口为主要业务端口，可通过配置限制相关被攻击端口的业务带宽。

d) 如部署了流量清洗设备，根据实际环境需要启动流量清洗。

参 考 文 献

[1] GB/T 20984-2022 信息安全技术 信息安全风险评估方法
[2] GB/Z 20985.2-2020 信息技术 安全技术 信息安全事件管理第2部分：事件响应规划与准备指南
[3] GB/T 20986 信息安全技术 信息安全事件分类分级指南
[4] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
[5] GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求
[6] GB/T 22239-2019 信息安全技术 信息系统安全等级保护基本要求
[7] GB/T 22240-2020 信息安全技术 信息系统安全等级保护定级指南
[8] GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范

电信终端产业协会团体标准

网络产品应急响应安全要求　技术要求

T/TAF 182—2023

*

电信终端产业协会印发

地址：北京市西城区新街口外大街 28 号

电话：82052809

电子版发行网址：www.taf.org.cn