应 急 响 应 预 案

**目** **录**

目录

[1 应急响应策略 3](#_Toc28285)

[2 安全事件分级 3](#_Toc12982)

[3 应急响应流程 4](#_Toc7372)

[4 职责分工明细 5](#_Toc8892)

[5 通用响应过程 5](#_Toc19204)

[5.1 DDoS 攻击事件 6](#_Toc20431)

[5.2 黑客入侵事件 6](#_Toc1211)

[5.3 重大系统漏洞披露 7](#_Toc10115)

[5.4 非网络安全相关事故 7](#_Toc6198)

[6 测试演练计划 7](#_Toc8677)

[7 维护更新计划 7](#_Toc31918)

[8 编写人 8](#_Toc9030)

[9 生效日期 8](#_Toc28505)

[10 签发人 8](#_Toc23934)

[附件一：安全事件处理人联系方式 9](#_Toc9767)

[附件二 ：安全事件处理记录单 10](#_Toc13390)

[附件三 ：安全事件学习记录单 11](#_Toc11552)

1 应急响应策略

为保障公司经营活动的持续安全运行，减少由信息安全风险产生的经济或名誉损失， 满足国家法律、法规对公司信息安全保障能力的要求。

本规定参考 《中华人民共和国网络安全法》、《数据安全法》 要求， 依据某某公司的信息安全现状进行设计、制定和编写。它的适应范围包括：组织——公司所有与业务相关的组织部门，人员——公司所有与业务系统相关的员工、第三方合作伙伴等，资产——所有对公司内部或外部提供服务的信息系统及相关资产。 它的目标是实现重要业务系统在发生生产事故后能够通过预案快速判断和决策，组织人员恢复和重建业务系统。它的核心原则是最大化减低损失， 保障人员和财产的安全。

本规定体现了公司管理者对业务连续性要求 ，它得到了公司管理者的充分认可并授权 自签发之日起在公司内部执行。

2 事件分级

|  |  |  |  |
| --- | --- | --- | --- |
| **级别设置** | **一般事件** | **严重事件** | **重大事故** |
| 业务对外完全停止服务时间 | 1-2小时 | 2-8小时 | 8小时以上 |
| 其他判断项 |  |  |  |

表 1. 安全事件分级标准

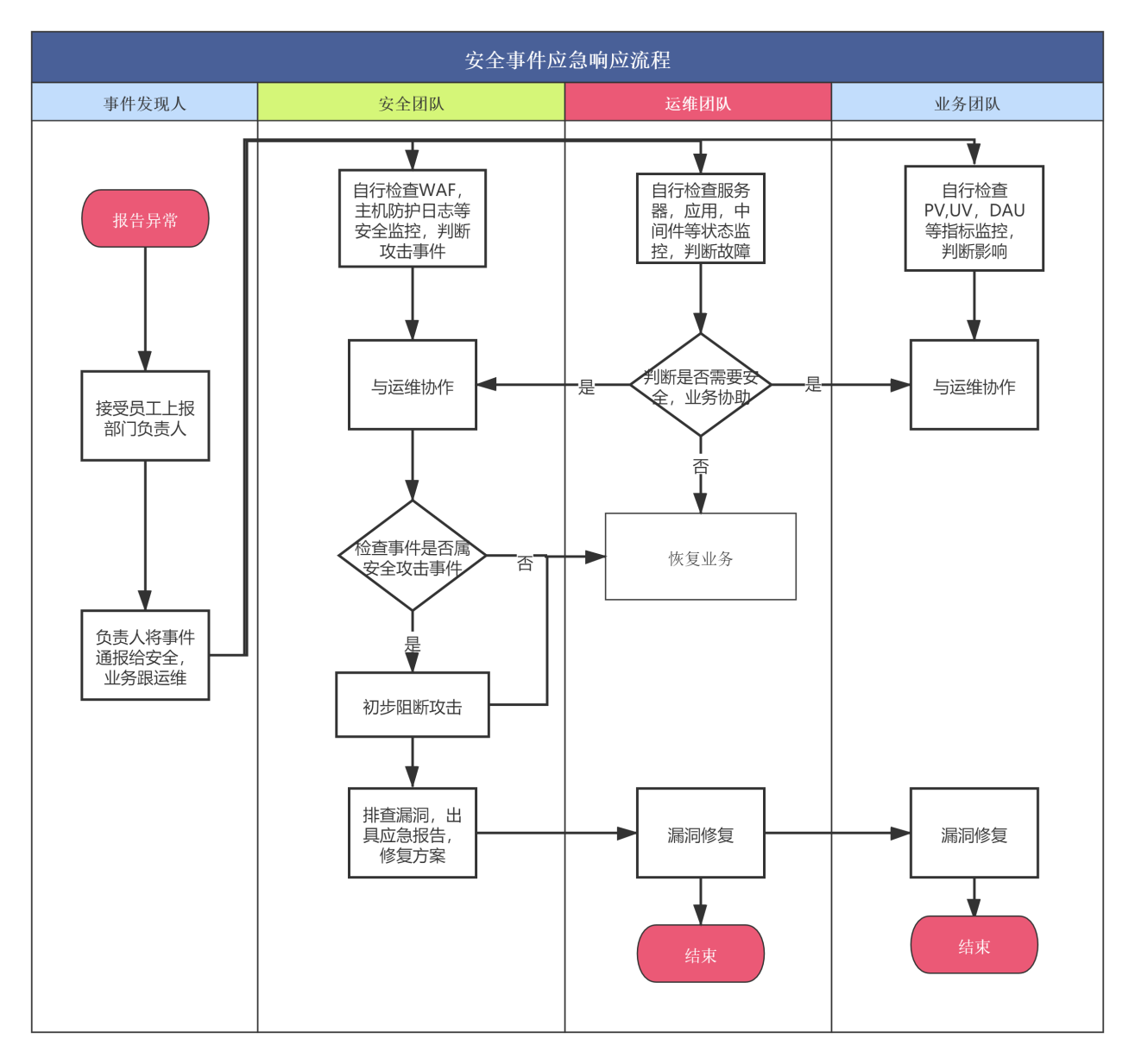
3 职责分工明细

■公司领导及业务负责人 ：领导本规定的制定并授权签发 ，在应急响应过程中确定系统、 信息和计划的优先级 ，组建临时的业务应急响应团队、保障恢复工作以最高效方式完成。

■安全团队 ：参与规定的制定和完善 ，和业务团队进行沙盘演练 ，协同应急响应工作。

■运维团队 ：根据预案或者是临时缓解措施对相关系统进行处理和恢复。

■业务团队 ：根据预案或者是临时缓解措施协助对相关系统进行处理和恢复。

4 应急响应流程

事件发现者上报事件，所属部门负责人将事件同步通知到业务团队，安全团队，运维团队。

三方团队分别围绕事件进行信息共享与相应排查。业务团队检查影响用户数量等，运维团队检查影响服务器与域名，安全团队检查事件类型，系统漏洞等。

确定事件非安全攻击后，由运维和业务方自行处理后续事务，安全团队不再跟进。

确定事件属安全攻击后，由安全团队出具建议、报告和方案。运维及业务团队根据此预案或具体建议、报告、方案进行相应处理，恢复业务运行。安全团队排查后出具排查报告，说明入侵原因漏洞、黑客行为意图、黑客行为影响等信息。运维团队及业务团队根据报告内容进行相关漏洞修复。

5 通用响应过程

依据国内外标准和要求，安全事件应急响应的通用过程为： PDCERF。

A ．准备（ Preparation ） 通过对公司网络的分析，采取必要的措施加强网络安全。

B ．检测（ Detection ） 分主动发现和被动发现两种途径。

C ．抑制（ Containment ） 对已经发生安全事件的主机， 通过边界控制设备对相关网 络或主机加以隔离，避免影响其它的主机或网络区域。

D ．根除（ Eradication ） 分析安全事件原因 ，确定事件危害程度， 采取防范措施， 完善企业信息安全策略。

F ．恢复（ Recovery） 包含对主机和网络控制的恢复。

G ．跟踪（ Follow-up ） 对安全事件进行总结学习，严重安全事故可申请司法保护。

下面是典型安全事件应急响应过程 ：

5.1 DDoS 攻击事件

当发生 DDoS 攻击事件时，后续过程如下：

■业务团队检查当前攻击是否影响业务运行，是否需要进行干预处理。

■需要处理时，业务团队、运维团队、安全团队分别进行相关流程，申请新高防资源。

■运维团队准备相应的新资源如服务器、IP等 ，高防资源管理者完成高防配置后通知 ；

■完成新环境配置后申请业务域名解析变更 ，域名管理员根据高防地址更新解析 ；

■如果源站IP依然被攻击，可镜像一套新源站环境，将新站接入高防，使用新环境提供

服务。

5.2 黑客入侵事件

当系统发生黑客入侵事件时，后续过程如下：

■协调网络、系统管理员对黑客攻击进行阻断 ，抑制攻击行为 ，防止影响扩大 ；

■业务团队检查系统数据， 用户数据有无被篡改等。运维团队启用新资源重新部署业务，将流量迁移到新资源上。安全团队收集服务器，域名，业务等异常现象，为下一步排查做准备 ；

■安全团队登录主机对系统、黑客攻击行为进行分析，确定黑客意图，给出意见说明域名，服务器，业务系统需要进行怎样的处理，并通知相关负责人 ；

■安全团队紧急查找漏洞并给出修复措施，出具应急响应报告，说明入侵原因，黑客行为意图，黑客行为影响等信息。

■业务团队根据报告进行相关处理、决定是否报告公安机关等。运维团队根据决定保留服务器镜像或重装系统。

5.3 重大系统漏洞披露

当发生大规模系统漏洞事件时，后续过程如下：

■业务线上报或安全团队从第三方平台获得重大系统漏洞资讯后启动应急响应流程 ；

■联合安全服务商对漏洞进行研究、测试和确认 ，在公司安全组织内发布安全通告 ；

■技术手段确定影响范围 ，和业务联动排查有漏洞历史记录的系统 ，跟踪 SRC 动态 ；

■技术手段升级网络入侵检测规则、及时感知黑客对我们业务系统的攻击情况。

5.4 非网络安全相关事故

当发生事件查明非网络安全相关时，后续过程如下：

■运维团队，业务团队合作恢复业务运行，安全团队不再主动跟进，待命协助 ；

■业务恢复运行后，由各相关方自行协商进行事件后续处理。

6 测试演练计划

演练先事先设定一个场景——可能会面对的场景，开始演练之前就确定好特定的参数 和演练的范围，测试团队必须在测试内容与如何合理决定成功与否方面达成一致。

■演练周期——至少应该对重要系统进行一年一次的演习。

■演练类型——模拟测试， 应急响应团队集中在一起执行应急响应计划。

7 维护更新计划

■每年应组织安全团队、 业务部门对本规定进行评审和更新以满足安全需求。

■发生重大安全事故后， 应组织安全团队、 业务部门对本规定进行评审和更新以满足 安全需求。

8 编写人

安全团队。

9 生效日期

2021 年 10 月 1 日。

10 签发人

CTO 某。

附件一：安全事件处理人联系方式

|  |  |  |  |
| --- | --- | --- | --- |
| 安全事件处理人联系方式 | | | |
| **部门** | **负责人**  （格式： 姓名+电话+办公邮箱） | **处理人**  （格式： 姓名+电话+办公邮箱） | **备注** |
| **系统管理** |  |  | 第一联系人 |
|  |  | 第二联系人 |
| **网络管理** |  |  | 第一联系人 |
|  |  | 第二联系人 |
| **数据管理** |  |  | 第一联系人 |
|  |  | 第二联系人 |
| **业务管理** |  |  | 第一联系人 |
|  |  | 第二联系人 |
| **测试管理** |  |  | 第一联系人 |
|  |  | 第二联系人 |
| **安全管理** |  |  | 第一联系人 |
|  |  | 第二联系人 |
| **资产管理** |  |  | 第一联系人 |
|  |  | 第二联系人 |
| **第三方** |  |  | 售后联系人 |
|  |  | 技术联系人 |

表 2. 安全事件处理人联系方式

附件二 ：安全事件处理记录单

|  |  |  |  |
| --- | --- | --- | --- |
| 安全事件处理记录单 | | | |
| **报告人** |  | **报告时间** |  |
| **记录人** |  | **记录时间** |  |
| **涉及设备** |  | **涉及系统** |  |
| **现象描述** ： | | | |
| **影响范围（业务和网络系统）** ： | | | |
| **事件级别** ： | | | |
| **处理记录** ： | | | |

表 3. 安全事件处理记录单

附件三 ：安全事件学习记录单

|  |  |  |  |
| --- | --- | --- | --- |
| 安全事件学习记录单 | | | |
| **主持人** |  | **学习时间** |  |
| **记录人** |  | **记录时间** |  |
| **事故起因** ： | | | |
| **触发原因** ： | | | |
| **损失类型** ： | | | |
| **事故发现及应对预案** ： | | | |
| **造成故障的服务** ： | | | |
| **受影响服务** ： | | | |
| **故障时间段** ： | | | |
| **是否自动恢复** ： | | | |
| **发现问题** ： | | | |
| **止损工作** ： | | | |
| **恢复工作** ： | | | |
| **通报工作** ： | | | |

表 4. 安全事件学习记录单