

# 网络安全风险 评估报告

巨桃游娱（天津）信息科技有限公司

## 目 录

一、概述 .....	3
------------	---

1.1 工作方法 .....	3
1.2 评估范围 .....	3
1.3 评估方法 .....	3
1.4 基本信息 .....	3
二、资产分析 .....	4
2.1 信息资产识别概述 .....	4
2.2 巨桃游娱系统架构图 .....	4
三、评估说明 .....	4
3.1 无线网络安全检查项目评估 .....	4
3.2 无线网络与系统安全评估 .....	5
3.3 ip 管理与补丁管理 .....	5
3.4 防火墙 .....	5
四、威胁细类分析 .....	6
4.1 威胁分析概述 .....	6
4.2 威胁分类 .....	7
4.3 威胁主体 .....	7
五、安全加固与优化 .....	8
5.1 加固流程 .....	8
5.2 加固措施对照表 .....	8
六、评估结论 .....	9

# 一、概述

巨桃游娱（天津）信息科技有限公司通过自评估的方式对网络安全进行检查，发现系统当前面临的主要安全问题，边检查边整改，确保信息网络和重要信息系统的安全。

## 1.1 工作方法

在本次网络安全风险评测中将主要采用的评测方法包括：人工评测、工具评测。

## 1.2 评估范围

此次系统测评的范围主要针对该业务系统所涉及的服务器、应用、数据库、网络设备、安全设备、终端等资产。

主要涉及以下方面：

- 业务系统的应用环境；
- 网络及其主要基础设施，例如路由器、交换机等；
- 安全保护措施和设备，例如防火墙、IDS 等；
- 信息安全管理体制。

## 1.3 评估方法

采用自评估方法。

## 1.4 基本信息

被评估系统名称	巨桃游娱
业务系统负责人	王瑞
评估工作配合人员	李世雷



制度、定期升级的安全策略、病毒预警和报告机制、病毒扫描策略（1周内至少进行一次扫描）。

### **3.2 无线网络与系统安全评估**

无线局域网核心交换设备、城域网核心路由设备应采取设备冗余或准备备用设备，不允许外联链路绕过防火墙，具有当前准确的网络拓扑结构图。无线网络设备配置有备份，网络关键点设备采用双电源，关闭网络设备HTTP、FTP、TFTP等服务，SNMP社区串、本地用户口令强健（>8字符，数字、字母混杂）。

### **3.3 ip 管理与补丁管理**

有无线IP地址管理系统，无线IP地址管理有规划方案和分配策略，无线IP地址分配有记录。有补丁管理的手段或补丁管理制度，Windows系统主机补丁安装齐全，有补丁安装的测试记录。

### **3.4 防火墙**

无线网络中的防火墙位置部署合理，防火墙规则配置符合安全要求，防火墙规则配置的建立、更改有规范申请、审核、审批流程，对防火墙日志进行存储、备份。

## 四、威胁细类分析

### 4.1 威胁分析概述

#### 4.1.1 外部威胁

来自不可控网络的外部攻击，主要指移动的 CMNET、其它电信运营商的 Internet 互联网，以及第三方的攻击，其中互联网的威胁主要是黑客攻击、蠕虫病毒等，而第三方的威胁主要是越权或滥用、泄密、篡改、恶意代码或病毒等。

#### 4.1.2 内部威胁

主要来自内部人员的恶意攻击、无作为或操作失误、越权或滥用、泄密、篡改等。另外，由于管理不规范导致各支撑系统之间的终端混用，也带来病毒泛滥的潜在威胁。

对每种威胁发生的可能性进行分析，最终为其赋一个相对等级值，将根据经验、有关的统计数据来判断威胁发生的频率或者概率。威胁发生的可能性受下列因素影响：

- 资产的吸引力；
- 资产转化成报酬的容易程度；
- 威胁的技术力量等。

下面是威胁标识对应表：

威胁等级	可能带来的威胁	可控性	发生频度
高	黑客攻击、恶意代码和病毒等	完全不可控	出现的频率较高（或 $\geq 1$ 次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过。
中	物理攻击、内部人员的操作失误、恶意代码和病毒等	一定的可控性	出现的频率中等（或 $> 1$ 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过。
低	内部人员的操作失误、恶意代码和病毒等	较大的可控性	出现的频率较小；或一般不太可能发生；或没有被证实发生过。

## 4.2 威胁分类

下面是针对威胁分类对威胁途径的描述，其中不包括物理威胁：

威胁种类	威胁途径
操作错误	合法用户工作失误或疏忽的可能性
滥用授权	合法用户利用自己的权限故意或非故意破坏系统的可能性
行为抵赖	合法用户对自己操作行为否认的可能性
身份假冒	非法用户冒充合法用户进行操作的可能性
密码分析	非法用户对系统密码分析的可能性
安全漏洞	非法用户利用系统漏洞侵入系统的可能性
拒绝服务	非法用户利用拒绝服务手段攻击系统的可能性
恶意代码	病毒、特洛伊木马、蠕虫、逻辑炸弹等感染的可能性
窃听数据	非法用户通过窃听等手段盗取重要数据的可能性
社会工程	非法用户利用社交等手段获取重要信息的可能性
意外故障	系统的组件发生意外故障的可能性
通信中断	数据通信传输过程中发生意外中断的可能性

## 4.3 威胁主体

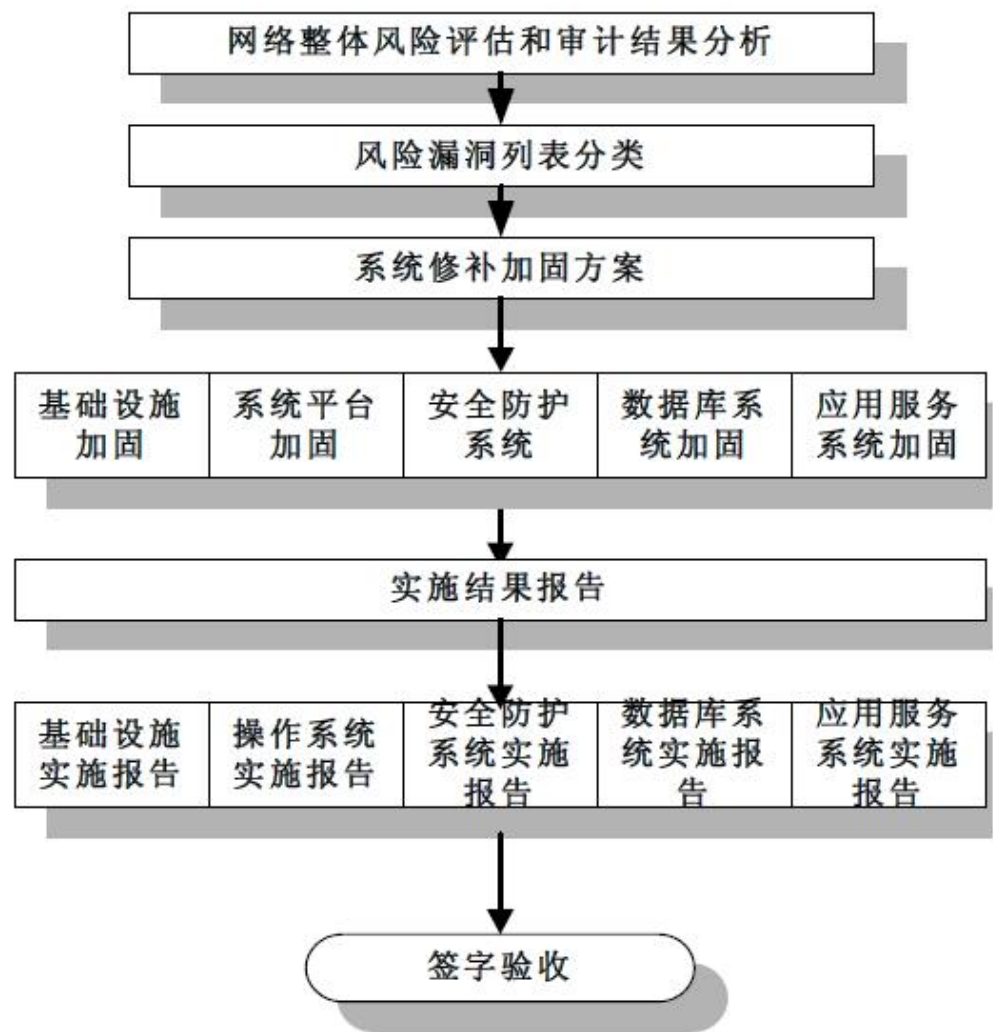
下面对威胁来源从威胁主体的角度进行了威胁等级分析：

威胁主体	面临的威胁
系统合法用户 (系统管理员和其他授权用户)	操作错误
	滥用授权
	行为抵赖
系统非法用户 (权限较低用户和外部攻击者)	身份假冒
	密码分析
	安全漏洞
	拒绝服务
	恶意代码
	窃听数据
	社会工程
系统组件	意外故障
	通信中断

## 五、安全加固与优化

### 5.1 加固流程

常规安全修复和加固服务主要依据以下流程：



### 5.2 加固措施对照表

项目	可能的影响和方式	等级	安全加固措施	备注
资产评估	资产信息泄露	高	合同、协议、规章、制度、法律、法规	
安全管理评估	安全管理信息泄露	高	合同、协议、规章、制度、法律、法规	
应急安全评估	系统切换测试导致部分业务中断、部分数据遗失	高	做好系统备份和恢复措施；通知相关业务人员在相应时间段注意保护数据，并检查提交的数据是否在测试后完整	可选



网络威胁收集	网络流量	低	控制中心与探测引擎直接连接。不占用网络流量	
网络/安全设备评估	误操作引起设备崩溃或数据丢失、损坏	高	规范审计流程； 严格选择审计人员； 用户进行全程监控； 制定可能的恢复计划。	
	网络/安全设备资源占有	低	避开业务高峰； 控制扫描策略（线程数量、强度）	
漏洞扫描	网络流量	低	避开业务高峰； 控制扫描策略（线程数量、强度）	
	主机资源占用	低	避开业务高峰； 控制扫描策略（线程数量、强度）	
控制台审计	误操作引起设备崩溃或数据丢失、损坏	高	规范审计流程； 严格选择审计人员； 用户进行全程监控； 制定可能的恢复计划。	
	网络流量和主机资源占用	低	做好系统备份和恢复措施	
应用平台	产生非法数据，只是系统不能正常工作	中	做好系统备份和恢复措施	
	异常输入（畸形数据、极限测试）导致系统崩溃	高	做好系统备份和恢复措施	

## 六、评估结论

公司依据国家、地方、行业相关安全法规、规范及标准，运用安全系统工程的理论及方法，对项目建设内容及安全管理，全面进行了现场查验、查证及综合性安全评价，总的来看，有了初步的安全基础设施，在管理方面具备了部分制度和策略，安全防护单一，技术上通过多种手段实现了基本的访问控制，但相应的安全策略、安全管理与技术方面的安全防护需要更新以适应要求。

需要对安全措施和管理制度方面进行改善,通过技术和管理两个方面来确保策略的遵守和实现,最终能够将安全风险控制在适当范围之内,保证和促进业务开展。