系统安全防护说明书

V1.0

免责声明：

本文档仅作为使用指导，针对当前版本生效。由于产品升级或其他原因，文档内容会不定期更新，恕不另行通知。

您购买或试用的产品、服务及特性应受北京潍鲸公司商业合同和条款的约束，文档中描述的部分产品、服务及特性可能不在您购买或使用的范围之内。

目录

1 前言

北京潍鲸科技有限公司是一家业务完全基于云计算的服务型公司，是一家面向企业级 IT/云服务公司，坚持以客户为中心，聚焦资源整合。潍鲸集成云厂商的工具资源、服务交付资源，推出针对各云厂商产品的服务解决方案，秉承开放、合作、共赢的原则，做好云生态的积极建设者，为企业用户提供全方位多选择的云服务模式。

潍鲸科技提供一站式运维服务解决方案，专为客户提供上云的咨询、设计、迁移、运维以及运营的云服务，其中包括上云的咨询设计、数据迁移、运维托管、大数据、混合云管理、安全以及集成服务等。为企业搭建云计算时代的 IT 基础技术框架及运维服务。

概述

本手册主要介绍潍鲸科技关于**系统安全防护说明书**。

注：本文下述北京潍鲸科技有限公司简称“潍鲸科技”

使用对象

安装实施人员、开发工程师、运维工程师。

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本变更记录

V1.0.0

2 系统安全

通过漏洞修复、防勒索、防病毒、防篡改、合规检查等安全能力，抵御恶意入侵，使用漏洞和配置检测消除系统弱点、预防恶意攻击，将网络入侵事件、Webshell、恶意软件、核心数据被加密勒索、DDoS 攻击事件、ECS 恶意肉鸡等行为进行实时监控。帮助您实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产和本地服务器并满足安全防护要求。

3 服务标准

3.1 木马查杀

用户网站如果一旦因安全漏洞出现挂马或者网站后门 webshell，将会给用户带来极大的安全风险，像 Webshell 通常是以 ASP、PHP、JSP、ASA 或者 CGI 等网页文件形式存在的一种命令执行环境，也称为网页后门。黑客在入侵网站后，通常会将 Webshell 后门文件与网站服务器 Web 目录下正常的网页文件混在一起；然后使用浏览器来访问这些后门，得到命令执行环境，以达到控制网站或者 Web 系统服务器的目的。

3.2 漏洞修复

漏洞指在操作系统实现或安全策略上存在的缺陷，操作系统软件或应用软件在逻辑设计上存在的缺陷或在编写时产生的错误。攻击者可以对这类缺陷或错误进行利用，从而能够在未获得授权的情况下访问和窃取您的系统数据或破坏系统。系统漏洞需要系统管理员及时处理并修复，否则将带来严重的安全隐患。针对以下漏洞问题进行的安全修复。

1) Linux 软件漏洞
2) Windows 系统漏洞
3) CMS 漏洞
4) 应用漏洞

3.3 挖矿病毒处理

挖矿程序会占用 CPU 进行超频运算，导致 CPU 严重损耗，并且影响服务器上的其他应用。挖矿程序还具备蠕虫化特点，当安全边界被突破时，挖矿病毒会向内网渗透，并在被入侵的服务器上持久化驻留以获取最大收益。

由于挖矿程序具有联动作用，在清理过程中会存在处理不及时或清理不干净导致挖矿病毒反复发生、出现恶意脚本替换系统命令，从而导致执行系统命令时触发恶意脚本执行。因此，需要在挖矿程序的一个执行周期内，尽快将被入侵服务器上的木马程序和持续化后门清理干净，否则容易导致挖矿病毒频繁复发。

3.4 网页防篡改

网页防篡可实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。

网络攻击者通常会利用被攻击网站中存在的漏洞，通过在网页中植入非法暗链对网页内容进行篡改等方式，进行非法牟利或者恶意商业攻击等活动。网页被恶意篡改会影响用户正常访问网页内容，还可能会导致严重的经济损失、品牌损失甚至是政治风险。

3.5 病毒防御

勒索病毒、挖矿程序等持久化、顽固型病毒已经成为网络安全最大的威胁。病毒防御功能针对此类病毒提供扫描、告警、深度查杀和数据备份的能力，可有效预防此类病毒入侵您的服务器。病毒防御功能针对勒索病毒、挖矿程序等持久化、顽固性病毒防护的所有服务器提供深度扫描服务。

1) 勒索病毒
2) 挖矿程序
3) DDoS 木马
4) 木马程序
5) 后门程序
6) 恶意程序
7) 高危程序
8) 蠕虫病毒
9) 可疑程序
10) 自变异木马

3.6 安全基线检查

病毒和黑客会利用主机存在的安全配置缺陷入侵主机盗取数据或是植入后门，常见的安全配置缺陷有系统或是网站及数据库服务的弱密码或是权限配置不当，基线检查能帮助您快速的对大量的主机进行扫描，发现包括系统、账号、数据库、弱密码、等级保护合规配置中

存在的风险点，并提供修复方式，助力您快速提升安全防线，同时满足包括等保二级、三级合规监管需求。

4 注意事项

1） 在服务过程中，需要提供云服务器的账号和密码，待服务完成后及时修改密码。

5 联系潍鲸

潍鲸科技为客户提供多种安装配置服务，可以根据用户需求提供定制化服务，为客户提供满意的服务，我们一直在努力。

北京潍鲸科技有限公司

网址：www.weijing.co

邮箱：support@weijing.co

电话：15718868001