

<<网络安全应急实践指南>>

图书基本信息

书名：<<网络安全应急实践指南>>

13位ISBN编号：9787121061943

10位ISBN编号：7121061945

出版时间：2008

出版时间：电子工业出版社

作者：CNCERT/CC,国家互联网应急中心

页数：240

字数：218000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<网络安全应急实践指南>>

内容概要

本书由国家计算机网络应急技术处理协调中心（简称国家互联网应急中心，CNCERT/CC）总结多年的工作经历和实践经验而写就。

内容包括有关网络安全应急的基础知识、应急组织的职能作用与日常运作、各类典型网络安全事件的处置办法、应急组织之间的协调合作与交流平台，以及网络安全文化的培育等内容。

本书属于实践指南或工作指导类的题材，结合并依据一定的理论基础，注重操作层面实践经验的总结和具体工作的介绍与指导，可作为相关从业人员的工具指导书，具有良好的实用价值。

本书适合各类应急组织、从事网络安全工作的系统和部门、从事网络安全工作的管理人员和技术人员阅读。

<<网络安全应急实践指南>>

书籍目录

应急响应 基础篇 1. 计算机安全事件 2. 应急响应的目标 3. 应急响应的能力要求 4. 应急响应组织 5. 应急响应方法 6. 计算机取证 应急响应 组织篇 第1章 应急响应组织及其作用 1.1 应急响应组织 1.2 应急响应组织的作用 1.2.1 网络安全事件应急响应 1.2.2 网络安全事件预防 1.2.3 安全质量管理 1.3 应急响应小组的分类、架构和工作范围 1.3.1 应急响应小组的分类 1.3.2 应急响应小组的架构 1.3.3 应急响应小组的工作范围 第2章 国家级网络安全应急响应组织 2.1 什么是国家级网络安全应急响应组织的职能 2.2 国家级网络安全应急响应组织需要具备的能力 2.3 国家级网络安全应急响应组织需要具备的能力 2.4 国家级网络安全应急响应组织与其他应急组织合作的意义 第3章 CNCERT/CC 3.1 CNCERT/CC简介 3.2 CNCERT/CC的职能和工作原则 3.2.1 主要职能 3.2.2 工作原则 3.3 863-917网络安全监测平台 3.3.1 具备的能力 3.3.2 发挥的作用 3.4 CNCERT/CC处置的典型网络安全事件 3.4.1 蠕虫事件 3.4.2 网络仿冒 3.4.3 拒绝服务攻击 3.4.4 僵尸网络事件 3.4.5 UDP1026和1027端口流量异常事件 3.5 CNCERT/CC与国内应急组织的交流与合作 3.6 CNCERT/CC的国际交流与合作 第4章 网络安全应急响应小组的日常运作 4.1 网络安全应急响应小组的建立 4.1.1 需求分析 4.1.2 提出建议 4.1.3 制定计划或方案 4.1.4 获得批准 4.1.5 获得所需的资源 4.1.6 正式运作 4.1.7 与其他网络安全应急响应小组建立联系 4.2 网络安全应急响应小组的工作原则 4.2.1 行为准则 4.2.2 信息分类原则 4.2.3 信息透露原则 4.2.4 媒体原则 4.2.5 安全原则 4.2.6 失误处理原则 4.3 网络安全应急响应小组运作的有关问题 4.3.1 网络安全应急响应小组的规章 4.3.2 工作计划 4.3.3 通信 4.3.4 电子邮件 4.3.5 工作流管理工具 4.3.6 信息系统 4.3.7 IP地址和域名 4.3.8 网络和主机的安全性 4.3.9 安全管理 4.3.10 现场响应 4.3.11 员工的问题 4.4 网络安全应急响应小组之间的协作 4.4.1 建立联系点(POC)网络 4.4.2 保证信息共享安全性 4.4.3 协作进行事件处理和调查 4.4.4 注册到一个公共目录服务 应急响应 实践篇 第5章 大规模蠕虫事件的处置 第6章 僵尸网络的处置 第7章 网站被攻击事件的处置 第8章 网络仿冒事件的处置 第9章 拒绝服务攻击事件的处置 第10章 不当使用事件的处置 应急响应 协作篇 第11章 网络安全应急响应的信息共享 第12章 FIRST组织 第13章 APCERT组织 第14章 关于网络安全应急年会应急响应 文化篇 第15章 培育网络安全文化 第16章 提高全民信息安全意识 附录A 缩略语解释 附录B 名词解释 参考文献

章节摘录

第2章 国家级网络安全应急响应组织 2.3 国家级网络安全应急响应组织需要具备的能力
为保障国家公共互联网等网络基础设施的安全运行，国家级网络安全应急响应组织必须具备以下的能力：
1. 网络安全监测能力 国家级网络安全应急响应组织首先应具备网络安全事件的监测能力，实现对网络安全运行情况的全方位监测。

为了保障有效的监测行为，国家级网络安全应急响应组织必须全面具有网络安全相关信息的获取能力，应能通过各种信息渠道与合作体系，及时获取如最新漏洞信息、蠕虫疫情爆发等各种安全事件与安全技术的相关信息；在获得相关信息后，还必须具备对安全信息进行分析判断的能力，应能对各类安全事件的有关数据进行综合分析，并形成权威性的数据分析报告。

2. 重大网络安全事件发现和预警能力 能综合分析、利用监测和其他渠道获取的网络安全信息，及时发现各类重大网络安全事件隐患和网络安全事件，并在必要的时候向有关应急组织和相关部门发出预警信息，以做好网络安全防范工作，直接减少网络安全事件发生的可能性，即使不可避免地发生了网络安全事件，也可以尽量降低和减少网络安全事件带来的损失和影响。

3. 重大网络安全事件的应急响应能力 在发生公共互联网的重大网络安全事件时，根据互联网行业主管部门——信息产业部发布的《公共互联网网络安全应急预案》中的规定，按“四级/一般”、“三级/预警”、“二级/肘良警”、“一级/紧急”的事件级别和分级响应流程进行网络安全事件的应急响应。

国家级网络安全应急响应组织则应充分发挥自身的技术手段和协调优势，借助已经建立的国内应急处理体系和国际合作渠道，对涉及公共互联网的重大网络安全事件进行技术协调和处置，尤其是跨运营商网络、跨境的网络安全事件。

<<网络安全应急实践指南>>

编辑推荐

本书属于实践指南或工作指导类的题材，结合并依据一定的理论基础，注重操作层面实践经验的总结和具体工作的介绍与指导，可作为相关从业人员的工具指导书，具有良好的实用价值。

主要包括：网络安全应急的基础知识，应急组织的职能与日常运作，各类典型网络安全事件的处理办法，应急组织之间的协调合作与交流平台，网络安全文化的培育。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>