<<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

<<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

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”、“二级肘艮警”、“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。

主要内容包括：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。

<<网络安全应急实践指南>>

版权说明