网络安全应急实践指南

网络安全应急实践指南_下载链接1_

著者:CNCERT/CC

出版者:电子工业出版社

出版时间:2008

装帧:平装

isbn:9787121061943

《网络安全应急实践指南》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。

《网络安全应急实践指南》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。《网络安全应急实践指南》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。

作者介绍:

前言

2001年8月8日，我们这个组织也就是CNCERT/CC（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，National Computer Network Emergency Response Technical Team/Coordination Center of China）成立了。成立之初，国内对于这样一个名称表现得相当陌生，但在国际上，CNCERT/CC的成立却是令人注目的。这源于我们组织英文名称中的一个缩写词——CERT（计算机应急响应组织），对于世界各个国家和地区的CERT组织来说，CNCERT/CC的成立无疑是一个好消息，不仅说明在中国又多了一个CERT组织，而且说明CNCERT/CC是一个能够代表国家参与国际CERT事务的国家级机构，填补了世界在该区域的一个空白。

如果说，六年前的我们更多的是在学习、借鉴、探索和实践，今天的我们则已经具备了一套较为成熟的运行框架、机制和流程，并以此为基础卓有成效地发挥着应有的作用。我们的定位决定了我们的业务具有一定的广泛性和综合性，或多或少地涉及到各种类型的CERT组织的业务，尽管如此，我们还是明确了我们的工作重点，即以“全网”安全为首要着眼点，在支撑信息产业部做好全网安全运行监测的同时，为国家关键基础设施及重要信息系统部门提供技术支持。正是这个原因，我们在本书中介绍的多为大规模或高危害性网络安全事件的处理办法和应对措施，希望能对尽可能广泛的互联网用户群体具有一定的借鉴意义。

根据我们的经验，做好网络安全工作不进行定岗定员是无法确保实效的，而应急响应工作更是如此，这也是世界上形形色色国家的、政府的、商业的、企业的、教育的、科研的CERT组织存在的理由。不管是否有明确的CERT职能部门，也不管是否有明确的专业CERT人员，我们相信在全国的各行各业和各级部门都一定有类似的部门或人员在从事着网络安全应急响应的工作。我们的书正是写给他们看的，我们尽力总结我们在这六年的实践当中所积累的经验，挖掘我们对于网络安全应急响应工作不断深化的理解，梳理我们经过无数次考察、学习、交流和培训而获得的知识，最后以十几名经验丰富的老同事的集体智慧和劳动编纂出本书。我们相信，本书的出版对于从事网络安全应急响应工作的人员具有普遍的指导意义，特别是对那些尚未建立CERT小组的部门来说，本书更能够指导他们如何有效地组建和运作一个CERT组织并开展工作。同时，我们还就网络上最典型和最具危害性的几类安全事件给出了比较具体的处理措施和建议，以帮助他们根据自身的情况有针对性地采取行动。我们也没有忘记就这些安全事件给终端用户提出安全建议，目的是希望非专业人员和普通读者也能够从本书中获益。

我们发现，自2005年开始，利用系统漏洞进行传播的蠕虫已经不再是安全事件中的独家主角，而以僵尸网络、间谍软件、身份窃取为代表的各类恶意代码逐渐成为最大威胁，同时，拒绝服务攻击、网络仿冒、垃圾邮件等安全事件仍然猖獗；此外，与政治纪念日和时政相关的网络攻击活动也时有发生，网络安全事件在保持整体数量显著上升的同时，也呈现出技术复杂化、动机趋利化、政治化的特点。根据中国互联网信息中心2007年7月公布的《中国互联网络发展状况统计报告》显示，截至2007年6月，我国上网用户总数为1.62亿人，上网计算机达到6710万台，网络用户和网络主机的数量仍然在持续增长，与此同时，电子政务、电子商务、网络游戏、网络博客等互联网业务正在快速扩展，新的操作系统、新应用软件不断投入使用，这些都导致大量人为主观疏忽和网络系统客观漏洞的存在。而黑客攻击动机已经从单纯地追求“荣耀感”向获取多方面实际利益和表达政治情绪的方向转移，黑客技术的发展也将重点放在网上木马、间谍程序、恶意网站、网络仿冒、僵尸网络等方面，因此，网络安全问题变得更加错综复杂，涉及范围将不断扩大。我们估计，由于黑客发动攻击的目的的转变，今后发生大规模的网络安全事件的可能性比较小，而以僵尸网络、间谍软件、身份窃取为代表的恶意代码，以及网络仿冒、网址嫁接/劫持类安全事件将会继续增加，因此，我们将继续对此类安全事件保持密切关注，对此类事件的处理力度也会不断加强。由于此类事件通常不会是单点孤立地发生，受到一次事件影响的往往涉及多个部门和个人，或者说，遭受一次事件威胁或危害的很可能是多个部门和个人，因此，我们非常希望所有牵涉事件中的相关部门和个人能够通力合作，尽可能迅速有效地处理事件，将事件可能会对各个部门和个人造成的不良影响降低到最小程度。这也是为什么我们在书中所描述的那些事件的处理过程会涉及那么多的部门或个人。无疑，了解了这些事件的处理过程将会有助于读者很快找

到正确的办法、途径和部门来解决问题。

本书将与《网络与信息安全》（清华大学出版社）教材共同列入信息产业部网络与信息安全技术培训认证项目（NTC-NISE）的教学体系中，作为信息产业部IT职业技术培训指定教材与广大读者见面。信息产业部网络与信息安全技术培训认证项目（NTC-NISE）是信息产业部全国网络与信息技术培训项目（NTC）的组成部分，是根据国家职业技术标准要求及国家对专业技术人员加强培训且须持证上岗等文件精神所推出的面向各行政、企事业单位及行业系统的专业技术人员、管理人员进行资格认证的培训项目，由国信高科技术培训中心（信息产业部批准设立的信息化培训认证机构）负责具体的运营工作。

实际上，本书的写就与我们的成长相关，而我们的成长得益于四年前国家公共互联网安全事件应急处理体系的确立。依赖于这个体系，我们得以在与各个合作单位和部门的互动中发展壮大并日趋成熟，我们这些年来所取得的工作成绩离不开体系中各个合作单位和部门的大力协助与支持，在此，我们要对所有的合作单位和部门表示衷心的感谢。很遗憾，限于篇幅原因，我们无法细数和列出所有的合作单位和部门，那会是一份相当长的名单。

感谢参加本书编写的其他同志：张雪浩（“前言、部分基础篇”的编写），刘洋、顾嘉（“第8章 网络仿冒事件的处置”的编写），宋轶南（“第9章
拒绝服务攻击事件的处置”的编写），吴冰、何松（“第2章
国家级网络安全应急响应组织”的编写）。

国家计算机网络应急技术处理协调中心

二〇〇七年八月

目录:

网络安全应急实践指南_下载链接1_

标签

网络安全

应急响应

应急

评论

网络安全应急实践指南_下载链接1_

书评

网络安全应急实践指南_下载链接1_