<<信息系统安全事件响应>>

图书基本信息

书名：<<信息系统安全事件响应>>

13位ISBN编号：9787030155375

10位ISBN编号：7030155378

出版时间：2005-6

出版时间：科学出版社

作者：李德全 苏璞睿 编

页数：221

字数：295000

前言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。
计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。
数字化的生存方式席卷全球。
农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。
古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。
电子政务、电子商务等各种信息化应用之花，在华夏沃土上竞相开放，炎黄子孙们，在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。
科学规律的掌握，非一朝一夕之功。
治水、训火、利用核能都曾经经历了非常漫长的岁月。
不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。
生产力的发展，为社会创造出许多新的使用价值。
但是，工具的不完善，会限制这些使用价值的真正发挥。
信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾御技能不足的情况下，损害着人们自身的利益。
世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。
传统社会存在的不文明、暴力，在信息空间也同样存在。
在这个空间频频发生的有些人利用系统存在的脆弱性，运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。
人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。
随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。
因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。
信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。
什么是信息安全？
怎样才能保障信息安全？
这些问题都是严肃的科学和技术问题。
面对人机结合，非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真的研究。
我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头土脸，自暴自弃，我们需要的是具有革命的乐观主义精神，坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

<<信息系统安全事件响应>>

内容概要

本书是《信息安全国家重点实验室信息安全丛书》这一。
本书主要介绍了与信息系统安全事件响应相关的关键技术和一些管理措施，以及在处理领先卢安全事件过程中的主要工作内容。
书中主要内容包括：各种攻击技术介绍；如何进行日常安全管理，降低安全事件的发性；如何检测入侵事件，及时发现问题；如何组建应急响应小组，防患于未然；应急响应技术与工具介绍；事件响应过程中各个阶段所要完成的主要工作等。
本书可作为计算机、信息安全、管理信息系统等专业的高年级本科生、研究生的教学参考书，也可供相关领域的科研和工程技术人员，尤其是安全管理人员和应急服务人员参考。

<<信息系统安全事件响应>>

书籍目录

章节摘录

插图：能够得到最有效的利用，避免应急响应体系由于受到错误报警、虚假报警、恶意扰乱、恶作剧等行为的干扰而影响响应的效率，从而导致无法对真正的信息安全事件做出及时、有效的响应处理，应该对突发的信息安全事件或异常状况进行初步分析和可靠性确认，以保证报警信息的真实有效；确认报告安全事件或异常状况的责任人，以确保事件报告的可追究性和不可否认性。
2.抑制在确认事件发生后，应采取措施抑制事件的进一步扩散。
应急抑制的目的是限制安全事件对受保护信息系统造成影响的范围和程度。
应急抑制是信息安全应急响应工作中的重要环节。
在信息安全事件发生的第一时间内对故障系统或区域实施有效的隔离和处理，或者根据所拥有的资源状况和事件的等级，采用临时切换到备份系统等措施降低事件损失、避免安全事件的扩散（例如蠕虫的大规模传播）和安全事件对受害系统的持续性破坏，有利于应急响应工作人员对安全事件做出迅速、准确的判断并采取正确的应对策略。
应急抑制分为物理抑制、网络抑制、主机抑制和应用抑制四个层次的工作内容。
在发生信息安全事件时，应根据事件准备的分析结果，综合利用多个层次的抑制措施，保证抑制工作的及时、有效。
3.根除在事件被抑制之后，通过对事件的分析结果，找出事件根源并彻底清除。
对于单机上的事件，可以根据各种操作系统平台的具体检查和根除程序进行操作；针对大规模爆发的带有蠕虫性质的恶意程序，要根除各个主机上的恶意代码，则是十分艰巨的一项任务。
很多案例的统计数据表明，众多的用户并没有真正关注他们的主机是否已经遭受入侵，有的甚至持续一年多，任由感染蠕虫的主机在网络中不断地搜索和攻击别的目标。
造成这种现象的重要原因是各网络之间缺乏有效的协调和统一管理。
应急根除分为物理根除、单机根除和网络根除三个层次。
为了保证彻底从受保护网络系统中清除安全威胁，针对不同类型的安全事件，应综合采取不同层次的根除措施。

编辑推荐

《信息系统安全事件响应》是由科学出版社出版的。

<<信息系统安全事件响应>>

版权说明