<<应急响应&计算机司法鉴定>>

图书基本信息

书名：<<应急响应&计算机司法鉴定>>

13位ISBN编号：9787302097273

10位ISBN编号：7302097275

出版时间：2004-11-1

出版时间：清华大学出版社

作者：汪青青,Kevin Mandia,Chris Prosise,Matt Pepe,付宇光

页数：400

字数：594000

译者：汪青青,付宇光

内容概要

周边安全技术的有效性和分析能力正在提高。
计算机司法鉴定技术也同样如此。
但是，未知因素是管理和分析计算机数据的人。
不管是执法官员、私人调查员、信息安全专家、顾问，或者是其他安全专家，成功防止和响应网络威胁的关键在于对计算机证据的合理鉴定、收集、保存和分析。
本书提供了有效响应突发事件、收集计算机司法鉴定证据和分析合适的日志、文件所必需的知识、技巧和工具。
这同时提高了各单位对突发事件的处理能力，或者事发前就汲取了教训。
一盎司的预防效果等于一磅的治疗。
另外，本书还介绍了如何获取可能留下痕迹的位置和可能的对调查目标的警告，从而可以帮助公司或司法部门调查员主动执行在线调查。
现在，公司的宝贵资料通常放在计算机中，这容易受到知识渊博的内部人员或机智的计算机黑客的攻击，他们可能敲诈你、贩卖信息，或将信息公布到Internet。
当然，如果需要处理敏感问题，那么在采取措施之前，应该咨询安全部门、律师、知识丰富的计算机司法鉴定咨询公司(最好有执法或情报方面的经验)或执法机构。
总而言之，每个信息安全专家——不管是系统管理员、调查员、顾问或者执法官员——都应该遵循本书的建议。
信息系统内忧外患，受过良好训练的协同保护、应急响应和司法鉴定分析团队对于所有要保护自身和财产免受网络威胁的组织而言，都是必需的。

作者简介

Kevin Mandia是Foundston公司的计算机司法鉴定部门的主管。
他领导计算机司法鉴定专业小组，在过去的一年中，着手处理了在电子商务和金融服务单位发生的超过30起的计算机安全事故。
他还协助美国空军、美国联邦调查局和其他执法部门来处理一些正在调查的案子。

<<应急响应&计算机司法鉴定>>

书籍目录

<<应急响应&计算机司法鉴定>>

版权说明