网络安全事件响应

Incident Response

[美] E. Eugene Schultz
Russell Shumway 著

中国教育和科研计算机网紧急响应组(CCERT) 段海新 等 译

New Riders

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

网络安全事件响应

[美] E. Eugene Schultz　Russell Shumway　著

中国教育和科研计算机网紧急响应组（CCERT）　段海新　等　译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

网络安全事件响应/（美）舒尔茨（Schultz,E.E.）（美）沙姆伟（Shumway,R.）著；段海新译.
—北京：人民邮电出版社，2002.5
ISBN 7-115-10204-X

I.网… II.①舒…②沙…③段… III.计算机网络—安全技术 IV.TP393.08

中国版本图书馆 CIP 数据核字（2002）第 019411 号

版权声明

网络安全事件响应

◆ 著 [美] E.Eugene Schultz Russell Shumway
译 中国教育和科研计算机网紧急响应组（CCERT）段海新 等
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67180876
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：16.75
字数：395 千字 2002 年 5 月第 1 版
印数：1-4 000 册 2002 年 5 月北京第 1 次印刷

著作权合同登记 图字：01－2001－5370 号
ISBN 7-115-10204-X/TP・2836
定价：35.00 元

内容提要

本书是指导网络与系统安全事件响应工作的一本宝贵的战略指南。全书首先介绍了事件响应、风险分析等概念及其相关概念之间的关系，然后对事件响应组的组建和管理、时间响应的组织提出了许多建设性的建议，提出了事件处理经典的六阶段方法。从技术方面描述了入侵跟踪技术、陷阱与诱骗技术、内部攻击的响应问题，并用三章的篇幅介绍了法律问题和取证问题，讨论了事件响应中的人性因素，最后讨论了事件响应的发展方向。

本书适合计算机系统、网络与信息安全的管理人员、技术人员，大专院校从事网络安全技术的研究生、教师等研究人员。特别是对于计算机安全事件响应组（CSIRT）、安全服务企业以及政府相关的管理部门，本书是市面上难得的一本战略指南。

译者序

随着计算机网络及应用的发展，针对计算机网络的各种恶意的攻击也越来越多，影响范围和造成的损失也越来越大。安全相关的事件响应（Incident Response）在网络安全体系结构中是不可缺少的重要环节，国际上这一领域的研究和服务已经开展了 10 多年，在中国也已经引起了政府、教育和学术、企业等各界的密切关注。

中国教育和科研计算机网紧急响应组（CCERT）是中国第一个网络安全事件的响应组织，隶属于清华大学信息网络工程研究中心，依托于中国教育和科研计算机网（CERNET），面向全社会提供与网络安全事件响应相关的各种服务。CCERT 还承担国家网络与信息安全领域重要的科研课题，同时承担清华大学网络安全学科的教学任务。

本书是指导网络与系统安全事件响应工作的一本宝贵的战略指南，必将对国内事件响应工作发挥重要作用。书中的事件响应方法学、响应组的组建和管理等章节的内容已经用于指导 CCERT 事件处理和管理工作。

因此，本书的内容具有很强的可操作性，是一本不可多得的实践指南，不仅对国内已经成立或即将成立的事件响应组有重要的指导意义，而且对政府、企业、教育和学术机构的网络安全管理工作有重要的参考价值。

本书的翻译工作是在 CCERT 部分成员的共同努力下完成的，凝聚着 CCERT 成员的辛苦劳动。参与本书翻译工作的成员主要包括 CCERT 的工作人员段海新博士、赵乐男助教，博士研究生杨峰、戴世冬，硕士研究生曹麒麟、温世强，清华大学法学院陈继梅硕士翻译并审阅了与法律有关的内容，最后曹麒麟硕士汇总并整理了本书的所有内容。

由于译者水平有限，时间有限，有不足之处希望读者批评指正。您的批评和建议是对本书价值的肯定和对我们工作的帮助。我们的联系方式：

邮政地址：北京市海淀区 清华大学中央主楼 306 房间

邮政编码：100084

值班电话：010-62784301　　传　　真：010-62785933

电子邮件：report@ccert.edu.cn　　主　　页：http://www.ccert.edu.cn

中国教育和科研计算机网紧急响应组（CCERT）　段海新

2002 年 3 月于 清华大学

关于作者

E. Eugene Schultz 博士　美国能源部计算机事件咨询能力（CIAC）组创始人和前任负责人，现在是Global Integrity 公司REACT 组——第一个商业性的事件响应组的技术支持。

Russell Shumway　网络安全公司（Network Security Corporation）智能与响应服务组主任，负责NSEC 安全事件的管理以及开放源码监控服务。Russ 以前的工作是Global Integrity 公司REACT 计划的技术负责人，曾经为大量客户处理过无数的计算机安全事件。这些客户包括从《财富》排名前100 名的公司到个人用户，为美国前10 大金融服务公司中的7 个公司、全球前50 名中的13 个公司提供咨询服务。他帮助设计和开发了Global Integrity 公司金融服务事件共享和咨询中心（FS/ISAC）。

Terry Gudaitis 博士　行为科学家和犯罪学家，在行为评估和特征描述（profiling）学科有12 年的研究与应用实践的经验。她从Florida 大学获得了文学硕士和哲学博士学位。1987 年起，她为学术界、本地法律执行机构、联邦机构和私营企业提供国内外的行为评估与特征描述服务。

Gudaitis 博士作为一名犯罪心理学家，在中央智能机构的反恐怖中心工作。目前，Gudaitis 博士负责行为/ 犯罪描述的整合以及Global Integrity 公司的计算机法律问题，Clobal Integrity 公司是国际科学应用公司（SAIC）的子公司。Gudaitis 博士提供咨询、人力系统评估、私营企业的特征描述分析服务。Gudaitis 最近在计算机心理学、行为学杂志发表多篇论文，在SecureComm98 会议上提出了“内部威胁”的概念，她是一位美国华盛顿区“计算机犯罪特征描述”的客座发言人，还是高技术犯罪调查协会的一名活跃会员。

关于技术审稿人

这些审稿人为本书开发的全过程贡献了他们宝贵的实践经验。本书在写作过程中，这些专业人员审阅了所有的材料，从技术内容到组织和流程。他们反馈的意见对于确保“事件响应”这本书满足读者对高质量技术信息的需求起到了关键作用。

Patrick“Swissman”Ramseier，CCNA，CISSP。是 SARAA 公司的首席安全技术官，SARAA（Secure Archive Retrieval Anytime Anywhere）专门致力于使用最新的光成像、互联网传输、所有权保护等技术，对全国范围内的传统档案存储，管理和检索信息。公司中的这一成熟的商业模型能以安全的方式进行改造、使其有新的活力。Patrick 从 UNIX 系统管理员起家，在过去的 13 年中，他涉足的领域包括：企业级安全设计、体系结构复查、脆弱性分析、VPN 支持、物理安全、网络和操作系统安全（UNIX-Solaris，Linux，BSD 和 Windows NT/2000），培训、研究与开发。他有商业的文学士学位，正在攻读计算机科学的硕士和博士学位。

Larry Paccone 是 Logicon/TASC 的国家首席系统安全分析师。既是技术领导又是项目经理，他在 Internet 和网络/系统安全领域有 8 年的经验。他曾经领导过几个网络安全项目，支持国家网络/系统安全研究开发实验室。在那之前，Larry 在分析科学公司（TASC）作为一个国家的安全分析师工作了 5 年，评估常规军事武装结构。他有信息系统领域的硕士学位、国际关系学硕士学位、以及政治学学士学位。他还完成了网络和系统安全、互联网、广域网、Cisco 路由/交换以及 Windows NT 领域的 8 项职业认证。

前　言

读这本书的许多人都已经知道一些有关安全相关事件响应的信息。这些事件通常称为“入侵”、“攻击”、“安全侵入”等，这些术语变得越来越普遍了。为什么？其中一个最重要的原因是，系统应用和网络变得越来越复杂，因此增加了防范的难度。Internet 持续空前的增长速度，攻击者可以从世界的任何地方扫描、探查，然后攻击连接在 Internet 上的系统。问题的综合复杂性是高级管理的趋势，这对安全相关事件的威胁也是明显的，就像谚语里所说的“鸵鸟把头埋在沙子里（译者：由于问题复杂而顾头不顾尾）”。

安全相关的攻击经常带来灾难性的后果。第二章风险分析讨论了安全相关事件可能造成的负面影响的类型以及每种影响的范围。我们不主张“天要塌了”，而是提出选择性的损失统计。但是我们相信，问题比许多人所意识到的要严重的多。国家基础设施几年来一直面临严峻的风险。比如，一些破坏者可以关闭或修改部分基础设施的最关键的控制系统，如能源生产和分配系统、航空交通控制系统等。我们对计算机的依赖性越来越强，但是没能严格地控制计算机和网络的安全。这种状态仍将持续，直到某些事件——一些令公众无比震惊的安全相关事件发生。这种事件可能是大量且长期的能量损耗，或者是由于某人控制了计算机而导致一架庞大的喷气式飞机坠毁。

如果公众不要求更好的安全，政府似乎并不认真地考虑计算机安全问题。公司似乎也不能更严肃地对待计算机安全问题，除非有股东的压力、严重安全相关事件引起重大损失，或者由于安全措施太差引起一连串的法律诉讼。

在安全相关事件发生时，高效响应的需求随着威胁级别的增加成比例的增长。这本书的主要目的是向读者传达他们需要知道什么，不仅是为了建立事件响应能力，还包括提高现有的事件响应能力。

这本书所提出的概念和原理不是我们凭空构造的简单的思想。作者在他们计算机和信息安全的职业生涯中，花费了大部分时间帮助大量组织机构的事件响应。来自我们第一手经验的案例包含于全书之中，同时，我们试图尽力提出模型、趋势、以及其他理论概念，鼓励读者从概念层次上考虑事件响应。我们所面临的问题是多方面的，单独的计算机科学和信息技术只能解决部分问题。人的方面是特别重要的，尤其是在处理内部攻击的问题上。本书提出

了事件响应的一个广泛的透视图，覆盖多种技术、程序、管理的和心理学信息。这一广泛的视野使得本书对于有技术背景和没有技术背景的读者都是适用的。

本书的组织

本书的每一章关注于事件响应的一个特定领域。章节的划分如下：

- 第一章，“事件响应简介”，覆盖诸如什么是事件响应、为什么需要事件响应、最初必须考虑的几类问题等。
- 第二章，“风险分析”介绍了可能发生事件的种类，可能导致的破坏的类别，风险分析和事件响应工作之间的关系。
- 第三章，“事件响应方法学”提出了事件处理的一个经典的6阶段方法：准备、检测、围堵（containment）、根除（eradication）、恢复和追踪。这一章还提出了使用这一方法学的原理和应用每个阶段的具体考虑。
- 第四章，“事件响应组的组建和管理”解释了怎样建立和维护事件响应组。
- 第五章，“事件响应的组织”，覆盖怎样准备事件响应。主要讨论怎样处理组织的多个部分和谋取内部的支持，怎样对付新闻媒体。还提出了在事件发生后怎样减少损失的建议。
- 第六章，“网络攻击的追踪”描述了互联网系统的入侵跟踪技术和其他相关考虑。比如怎样开发通信信道，使相关人员能够获得所发生攻击事件相关的信息。
- 第七章，“法律问题”围绕事件响应领域及其适用性，讨论法律方面需要考虑的事项，包括诸如应用法律条例、个人隐私相关的考虑、事件响应相关的法律风险、怎样和法律执行团体打交道等。
- 第八章，“取证（I）”包括查找证据、辨别证据的形式、证据在审讯时的使用、最好的惯例、证据收集和证据分析隔离、取证处理和保存以及每种方法的技术和原理的应用场合，取证分析对证据获取的代价、数据取证和证据在法庭的使用或训练有素的听取诉讼以及其他重要的问题。
- 第九章，“取证（II）”继续第八章留下的问题，包括计算机取证方面更技术化的细节，包括隐蔽信道搜索、高级搜索、怎样处理加密数据、针对膝上型电脑特殊的考虑、老的系统、UNIX 主机、Linux 主机。
- 第十章，“事件响应中人性的因素”（由 Terry Gudaitis 博士编写，一个专门从事计算机犯罪研究的犯罪学家）讨论人性因素，包括怎样构造个人行为的特征描述，计算机犯罪发生后怎样会见嫌疑人。
- 第十一章，“内部攻击的响应”包括内部人员的种类、攻击类型、关于内部攻击的特殊考虑、怎样处理人际关系、法律和限制内部攻击案例到一个合适的范围之内的其他职能，以及内部调查与法庭听证之间的关系。

- 第十二章，“陷阱与诱骗手段”描述了几种可用的诱骗手段，怎样配置、建议，怎样衡量投资与收益。
- 第十三章，“事件响应的未来发展方向”，讨论事件响应未来将会是什么样子，以及对事件响应团体可能的影响。
- 附录A，“RFC-2196”包括专门针对事件响应的RFC。
- 附录B，“事件响应与报告检查列表”，提出了一个用于报告安全相关事件的样表。

我们相信，本书对您处理安全相关事件响应的挑战具有重要价值。

目 录