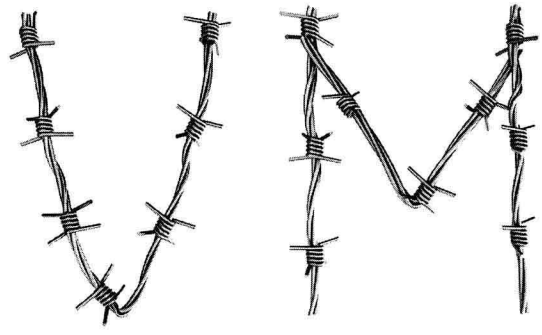
安全技術大系
SECURITY



Vulnerability Management

漏洞管理

（美）Park Foreman 著
吴世忠 郭涛 董国伟 张普含 译

机械工业出版社
China Machine Press

本书是资深安全漏洞管理专家、信息安全战略专家兼国际安全顾问20余年跨国工作经验的总结，以创新的方法从多个角度全面讲解了漏洞管理的理论、方法与最佳实践！结合大量实际案例深入阐述了安全漏洞防范的战略视野和实施方法，旨在帮助读者从技术、流程和管理的角度全面了解漏洞管理，从而掌握评估和减弱内外部漏洞的行之有效的方法。

本书共分10章：第1章介绍了风险管理、漏洞管理、安全产业现状等；第2章讲解漏洞产生过程、漏洞程序的作用，并结合实际案例讲解漏洞管理程序故障问题；第3章讲解漏洞管理计划的参与者、漏洞管理策略及合规性；第4章侧重于漏洞扫描的总体架构，并涵盖当前流行的漏洞管理技术，以及漏洞测试相关的数据、评价、技术标准和漏洞管理扫描程序Nessus；第5章阐述了如何选择漏洞管理产品，包括总体要求、实施过程的自动化、体系结构、如何进行用户定制与整合、评分和部署方法、访问控制等相关技术；第6章讲解漏洞管理流程，包括与漏洞管理相关的ITIL-ITSM过程和IAVA过程，以及该流程中的数据分级和风险评估等重要步骤；第7章介绍了一系列与执行、汇报、分析相关的文档，如发现报告、审计报告、合规性报告等；第8章提供了一些建议，引导读者从制定检查表、工程规划和实施策略等方面逐步了解如何在一个大型的公司里开发一个完整的漏洞管理项目；第9章从一个更宏观的、策略性的层面来研究漏洞的呈现形式及修复方法；第10章对上述内容进行了概括性总结。

图书在版编目（CIP）数据

漏洞管理 /（美）福尔曼（Foreman, P.）著；吴世忠等译 . —北京：机械工业出版社，2012.12
书名原文：Vulnerability Management

ISBN 978-7-111-40137-7

Ⅰ . 漏…　Ⅱ . ① 福…　② 吴…　Ⅲ . 企业管理 – 风险管理　Ⅳ . F270

中国版本图书馆CIP数据核字（2012）第248180号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：高婧雅
北京京师印务有限公司印刷
2013年1月第1版第1次印刷
186mm×240mm • 15.75印张
标准书号：ISBN 978-7-111-40137-7
定价：69.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

译 者 序

随着信息技术的飞速发展，互联网日益成为人们生活中不可缺少的一部分，社交网络、微博、移动互联网、云计算、物联网等各种新技术、新应用层出不穷。但不管是Facebook、Twitter等新兴互联网公司的迅速崛起，还是Android日益成为智能手机市场的主流操作系统，信息安全一直都是永恒的话题。“震网病毒”和“火焰病毒”事件凸显了网络武器的实战破坏能力，关键信息基础设施保护已成为世界各国网络空间防御的新重点；“维基泄密”事件彰显网络空间攻防双方的不对称性，“百密难免一疏”成为保密防范永远的痛；究其根源，所有这些信息安全事件都存在一个共同点——信息系统或软件自身存在可被利用的漏洞。因而，漏洞分析和风险评估日益成为信息安全领域理论研究和实践工作的焦点，越来越引起世界各国的关注与重视。

为推动国内的漏洞分析和风险评估工作，提高国家信息安全保障能力和防御水平，中国信息安全测评中心长期跟踪和关注相关领域的理论进展和技术进步，有针对性地精选一些优秀书籍译成中文，供国内读者参考借鉴。

本书从基本概念、重要作用、关键技术、流程管理等多个角度深入阐述了漏洞管理的运作及其发挥的作用。基本概念部分以风险管理的作用和漏洞管理的起源为切入点，分析了信息安全产业目前存在的缺陷及挑战，以及漏洞的诸多来源，并通过具体实例展现了失败的漏洞管理带来的巨大损失，进而说明了漏洞管理对于企业的重要

作用；关键技术部分介绍了多种实用的漏洞管理技术，包括主动和被动扫描、漏洞测试数据标准、漏洞严重等级标准、美国国家漏洞库（NVD）等，这些技术可以有效辅助漏洞管理工作的开展，极大提高管理效率；流程管理部分，阐明了以信息技术基础架构库–IT服务管理（ITIL-ITSM）流程和保障漏洞预警（IAVA）流程为基础的漏洞管理过程，以组织和规范漏洞管理工作，并深入介绍了此过程中形成的各类报告的形式和内容，最终说明了更高层面的策略性漏洞的管理方法。

本书翻译工作还得到了中国信息安全测评中心的章磊、王眉林、贾依真、吴健雄、张翀斌等同志的支持和帮助，在此深表感谢。

本书得到中国信息安全测评中心“漏洞分析与风险评估”专项工程、国家自然科学基金项目（90818021、61100047、61272493）的支持。

前　言

漏洞管理（Vulnerability Management，VM）已经有了上千年历史，城市、部落、国家和企业都会触及该学科的知识。漏洞会让潜在的攻击者有机可乘，任何机构的成功管理和运作都依赖于对漏洞进行检测和修复的能力。以往，人们修筑城堡，在城市中建造防御设施和高级预警系统，这些都是他们意识到自身的脆弱性并为了抵御危害而采取的各种措施。如今，我们检测到在软件系统、基础设施以及企业战略中也都存在一些漏洞，这些漏洞通常需要从多个角度、以创新性的方法来解决。

本书是一本信息安全从业人员的指导手册，读者包括安全工程师、网络工程师、安全部门的官员或首席信息主管（CIO）等在内的安全行业从业人员，系统地介绍了什么是漏洞管理及其在组织机构中的作用。本书涵盖了漏洞管理的各个重点领域以满足不同读者的需求。技术章节从宏观视角介绍了漏洞相关内容，不打算太纠结于技术细节的决策者也可以读懂这部分内容。其他有关流程和策略的章节，也能为领导层提供一定的参考，但主要是从工程师或安全主管的角度介绍了漏洞管理技术及其流程在企业中所起的作用。

作者建议对漏洞管理领域感兴趣的读者阅读相关章节，并略读其余章节。如果不能以长远的眼光全面理解漏洞管理的各个方面，将难以有效参与漏洞管理的任何一个环节。通常，员工们会担心他们在某个过程中承担的工作看起来毫无意义。希望本书介绍的内容能够在一定程度上减轻这种焦虑。

致谢

nCircle 网络安全公司的 Tim Erlin 先生着重从完整性和准确性角度审阅了技术相关章节，他所提的建议见解深刻，对我有很大的帮助。Ben Rothke 先生着重从清晰性角度协助审阅了原稿。

目　录

第1章

绪　论

漏洞管理（Vulnerability Management，VM）是对漏洞进行检测、分类、修复和消解的一种周期性活动。这是从公司或政府部门的角度所给定的比较宽泛的定义，在本书中将做进一步的讨论。漏洞管理并不是一门新兴的学科，也不是一门新兴的技术，其重要功能已被军事部门和私营企业普遍应用，主要用于对信息系统、流程和策略方面的漏洞进行检测并加强防御。随着组织的日益复杂，有必要将漏洞管理的功能完整地抽取出来，辅之以相关的支撑工具以使其成为一项专门的业务。这样一来，漏洞管理作为风险管理的一个部分将获得更为精确的定义。

1.1 风险管理的作用

风险管理旨在检测出可能发生损失的情况或事件，并获取相应的风险应对方法。有以下几种应对风险的方式：

- 接受风险，即什么也不做，让它发生。众所周知，这是养虎为患。
- 防范风险，即采取措施防止风险发生。
- 降低风险，即采取相应的保护措施来减轻风险造成的后果。

在漏洞管理中，我们看到风险都是由信息系统、流程和策略中的缺陷导致的。下图显示了漏洞管理与风险管理项目之间的关系。可以看出，漏洞管理在风险管理项目中的作用，是为了在组织的控制或影响下，发现并化解由漏洞导致的风险。风险管理中有关事件概率分析（event probability analysis）和持续性管理（continuity management）等其他方面，与漏洞没有直接关联。

漏洞管理通常关注软件技术漏洞和系统配置漏洞。而需要风险管理师关注的是那些无法被自动检测到的，与企业策略、经济状况和环境条件等相关的漏洞。这些漏洞存在于业务流程、策略和供应链等各个环节。业务中的每一项活动或策略，只要存在设计缺陷或适应性缺陷，就能被利用。因此，风险管理师更为重要的任务就是发现和应对这些挑战。在本书中，我们将主要讨论第一种类型的漏洞，同时也会对第二种类型的漏洞予以关注。

漏洞管理在风险管理体系中的角色

1.2 漏洞管理的起源

漏洞管理已经存在了很长时间但鲜有人关注，直到最近才引起人们的重视。长期以来军队都非常明白漏洞管理的重要性，并一直通过训练，不断完善漏洞管理。从组织和策略部署到各个士兵及武器的防御检查，其目的与审计是一样的。反复的训练、装备以及防御重组都是一种修复和改进。但如果不了解敌情，所有这些活动都无从谈起。

一个学过军事历史的学生能够很容易认识到交战的一方是如何利用对方的弱点和策略失误打败对方的。人们往往倾向于将这些胜利者誉为天才，而不会认为是失败者缺乏能力。例如，在坎尼战役中，汉尼拔撤退中线兵力，包围了罗马军队，从而从四面发起进攻，最终击败了罗马军队。由于这一经典战术，汉尼拔被视为战争天才。然而，人们还可以把这场战役看成汉尼拔的对手——罗马执政官之一的瓦罗（Varro）的策略失误。瓦罗原本相信罗马军队能够从中部突破汉尼拔部队的前线部队，从而将敌人的整个防线击退到他们身后的河流处，谁料汉尼拔竟然会改变前线阵型，假装撤退部队中部以诱敌。在战争中，保持部队行进统一是一项基本的军事纪律，但是瓦罗完全没有考虑这些，而这是一个漏洞。

然而，在商业领域里，人们总是倾向于认为应对风险的失败是能力不足的体现，尤其是当公司强大、富裕，能投入足够的资源解决风险时，这种观点尤为突出。

作为IT领域的一个学科，漏洞管理的发展尚不够成熟，用户也缺乏应用经验，这是因为之前一直没有强大的、企业级的技术可用；并且，以前人们也未充分认识到一个完整的、集成的、有着精确的流程定义的解决方案的必要性。虽然在企业环境下军事化的纪律可能不是必需的，但缺乏规范将可能导致某个关键的漏洞没有发现或没有补救，并可能最终导致灾难性的损失。

1.3 安全产业及其缺陷介绍

企业和政府一样都是依靠新产品来保证他们的网络安全，这种情况并不少见。安全产业因此一直致力于销售需要不断进行升级和维护的产品和服务。当某个安全问题出现端倪时，供应商早已开发出相应的解决方案。当用户开始滥用网络端口登录远程服务器时，供应商为我们提供了防火墙。当病毒成为一个不容忽视的问题时，供应商立刻又提供了反病毒软件和服务。当类似震荡波的蠕虫病毒出现后，供应商又在反病毒软件中增加了更多的网络防病毒功能。当企业内部的应用程序成为受攻击对象后，应用级防火墙又应运而生了。

不幸的是，这些解决方案似乎都治标不治本。大多数安全问题都是由于没有以安全的方式进行编码、修复、配置或设计而导致的。这就好比军队缺乏指挥官的监管、训练和充足的武器装备。技术供应商不断为我们提供产品化的解决方案，就好比将可以买到的全部武器都交给部队，但敌人并不会把武器作为攻击目标。由此可以购买安全产品是一种失败的策略。

我并非有意贬低各种安全技术产品的使用。安全技术产品是一个完整的安全策略的重要组成部分。但是，当各种安全问题发生时，很少有人会认真去检测和修复被利用的漏洞，而这些安全技术中没有一项能够完全补救诸如没有使用强密码或没有为所购买和安装的套装软件打补丁之类的漏洞带来的风险。

大多数网络安全产品的价值在于在没有出现更持久、更可靠的风险应对方案时，这些安全产品能够暂时地降低风险。安装反病毒产品是一个不错的选择，只要你进行及时、正确地更新即可。当新型病毒出现时，产品应当迅速做好准备防止该病毒入侵，直到病毒所攻击的软件供应商提供补丁。否则，最终病毒将寻找到攻入组织、突破防御的方法。因此，重要的是在这些发生之前对漏洞进行永久性修复。

1.4 来自政府和产业的挑战

IT企业面临着来自世界各国政府的挑战。不同的国家立法标准都不尽相同，使得企业在法律中常常遇到“雷区”，给一些操作带来了挑战，而跨国公司面临的挑战尤其巨大。在一些国家中，监管机构和工会组织，认为它可能会侵犯隐私。在一些国家，采集指定用户的上网行为记录是强制性的，并必须按照要求提供给政府。一些模糊而繁杂的规定，如美国的Sarbanes-Oxley（SOX）法案，已经形成了众多见效甚微但投入费用可观的安全控制措施。这使得基于全球管理软件包的网络主动防御面临更大的挑战，因为安全管理者现在只能从那些真正安全的行动中挑出符合当地法规的部分予以实施。

有关安全控制及相关认证和审计的行业标准越来越多，这些行业标准包括：SAS 70、SOX § 404、ISO 17799、ISO 27001、PCI、FIPS、HIPAA、GLB、IEEE P1074、EAL。标准和认证固然重要，但它们往往让我们忽略了最核心的问题：存在漏洞的软件、架构和策略。没有什么能长期替代基于良好编程、充分测试、合理配置并经有效实践后部署的软件是无法代替的。

1.5 漏洞的来源

对于软件购买者而言，软件公司自身就是一个真正的挑战：它们的编码水平和基础设计能力都应该持续改进。一些公司希望销售更多的产品，所以他们不断推出更多的功能，而不是去提高前期代码产品的安全性。他们可能开发了一种新的电子通讯协议或一项使用该协议的新应用，但他们却从没有在一开始就试着确保该协议的安全。在及时将漏洞告知用户和发布补丁方面，软件供应商的表现也并不令人满意。这是由于在软件供应商看来，打补丁是一件得不偿失的工作，因为没有人会为这些额外的开发工作埋单。由于缺乏内在动力，上述问题难以解决。在某些情况下，部分供应商可能在市场中处于绝对的垄断地位，消费者很少有其他选择。在这种情况下，更换软件制造商代价巨大，因为公司可能已在数千个结点部署了该软件，数百名训练有素的技术支持工程师也已经只熟悉该软件。

1.6 有缺陷的漏洞管理示例

当人们在落实漏洞管理措施时，通常不太认真。例如，某公司为符合支付卡行业

（Payment Card Industry，PCI）标准的规定，打算在整个企业中部署漏洞管理代理软件。该公司之所以这么做仅仅是因为审计人员告诉他们应该这么做，于是他们就做了，完全不考虑这项措施能够带来的收益和实施的效果。这样一来，唯一的有形要求就是这项已部署的技术，但没有人思考接下来的事情，例如这些显而易见的问题："我们应该在哪些主机上安装漏洞管理代理软件？""首先应该修复什么样的漏洞？"等。我把这种做法称为复选框安全策略（check box security strategy），即经公司授权的某个人向公司提供一份任务清单，然后公司就对照执行，每完成一项就在上面打钩。

复选框安全策略的另一个明显问题在于，能解决造成众多漏洞的根源的某个工具却没有正式的负责人。在上述例子中就体现为，代理软件和服务器安装后却没有指定任何人负责维护它们。不管用什么办法，系统是无法自行维护的。所以需要有人查看系统报告，修复或重装组件或代理软件，并确保报表服务器处于良好的运行状态。还需要有人负责监控整个系统，确保系统能达到预定目标。这和军队部署是类似的，如果没有指挥官的监管，部队就难以协调一致地行动。

1.7 漏洞管理的重要性

对于企业而言，资源是有限的，不可能取消在风险管理上投入太多的资源，因此前期的风险分析非常重要。但是，这不应该成为不进行漏洞管理的借口。当未实施漏洞管理时，在入侵检测或安全事件管理上花费有限的经费似乎难以自圆其说。尽管漏洞管理涉及更复杂的流程和系统，但能十分有效地降低企业面临的风险，而当企业需要防范的致命风险减少时，企业面临的风险状况将完全不同。

本书并不仅仅只是简单地介绍了漏洞管理技术和一些操作技巧，而且还从技术角度和流程角度深入讲解了漏洞管理是如何运作和发挥作用的，这两个方面相辅相成，缺一不可。技术工具在漏洞管理过程中起到推动作用，本书将花大量篇幅让读者体会到这一点。当在公司环境中实施了漏洞管理后你会发现，要实现安全真正需要的是那些愿意并且能够严格保证公司基础设施稳固性和安全性的人，除此之外的一切都是在浪费金钱和时间。

在本书中，你还将深入理解漏洞以及漏洞控制的策略意义。漏洞不仅存在于单个主机或是网络设备中，还可以存在于其他层面，这些层面中的漏洞必须通过调整技术战略才能予以解决。处于组织和行业层面的漏洞管理则属于风险管理的范畴了，已经超出了任何技术领域。

第2章

漏洞体验