<<政府网络与信息安全事件应急工作>>

图书基本信息

书名：<<政府网络与信息安全事件应急工作指南>>

13位ISBN编号：9787506665605

10位ISBN编号：7506665603

出版时间：2012-1

出版时间：中国标准出版社

作者：钱秀槟　等编著

内容概要

本丛书从电子政务的固有特点出发，结合编者单位丰富的实践经验，围绕电子政务信息安全保障的重点领域，介绍了信息安全的实用技术方法。

本书为丛书的应急分册，共分为8章。
分别介绍了突发事件的背景，当前针对各类突发事件的应急管理，网络与信息安全应急体系的主要内容，网络与信息安全事件的基础知识及其分类分级，网络与信息事件应急响应的流程，4类最典型事件的应急处置，网络与信息安全事件应急预案的编制方法，网络与信息安全应急的宣传、培训和演练工作。
本书还收录了相应的重要文件和部分可参考的范文。

本书可供各级政府以及安全服务机构、第三方测评机构从事信息化、网络与信息安全的管理和技术人员使用，也可供其他行业相关人员参考。

<<政府网络与信息安全事件应急工作>>

书籍目录

章节摘录

版权页： 插图： 步骤一，判断是否由于遭受域名劫持造成网页被“伪”篡改。
域名是否被劫持的决断方法较为简单，可直接用操作系统的ping命令实现，如果ping命令返回的IP地址信息与实际不一致，则通过正确的IP地址访问受害网站，检查网站内容是否正常。
当确定是由于域名系统遭受攻击而造成域名解析被错误定向，则应及时修改域名服务器的相关解析数据，并检查域名服务器是否遭受攻击。
同时，对于大型门户网站，还应尽量协调运营商，及时将各重要公共域名解析服务器中错误的域名解析缓存记录清除，以降低事件造成的影响。
步骤二，判断是否由于遭受局域网ARP攻击造成网页被“伪”篡改。
分析网页篡改是否是由于本地局域网ARP攻击所致，则应从两个方面进行检查。
一是直接本地登录网站所在服务器，从本地访问网站，检查网页内容是否被篡改；二是使用网络协议分析工具，检查局域网是否存在异常的ARP数据报文。
当确定局域网ARP攻击是造成网页篡改的原因，则应定位局域网中实施ARP攻击的主机。
步骤三，分析日志，确定攻击方式。
确定攻击方式是事件根除的前提，日志分析是确定攻击方式的最可靠的方法。
通过分析Web日志、网络审计H志，可以对通过Web应用系统实施攻击进行准确判断；通过分析系统日志、网络审计日志，可以对通过主机系统实施攻击进行准确判断；通过分析内容管理系统日志，可以对通过内容管理系统实施攻击进行准确判断。
根据分析确定得到的网页篡改方式，有针对性地从管理和技术上采取措施，避免事件再次发生。
步骤四，检查漏洞。
当因日志保存不完整，或者无法从日志中获知网页篡改的途径时，则只能通过检查漏洞来尝试处置。
漏洞检查的范围应包括可能的各个方面，如网站所在主机系统的安全漏洞、网站应用代码的安全漏洞、网站内容发布系统的安全漏洞等。
主机系统安全漏洞可以使用通用的漏洞扫描工具来检测，应用代码安全漏洞可以通过应用程序黑盒或白盒扫描工具来检测。
对扫描发现的各类安全漏洞进行必要的修补后，重新恢复网站系统运行并加强监测，以防止事件重复发生。
步骤五，综合分析。
当未发现任何已知的安全漏洞，或在完成对已发现漏洞的修补后，监测发现篡改事件重复发生，则本次事件可能是利用未知漏洞实施的，而要判定事件的最终原因，就需要进行更加全面的综合分析。

编辑推荐

《政府网络与信息安全事件应急工作指南》可供各级政府以及安全服务机构、第三方测评机构从事信息化、网络与信息安全的管理和技术人员使用，也可供其他行业相关人员参考。

版权说明