ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29766—2013

信息安全技术　网站数据恢复产品技术要求与测试评价方法

**Information security technology—
Technical requirements and testing
and evaluating approaches of website data recovery products**

2013-09-18 发布　　2014-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中华人民共和国
国家标准
信息安全技术 网站数据恢复
产品技术要求与测试评价方法
GB/T 29766—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.75 字数 78 千字
2013年10月第一版 2013年10月第一次印刷
*
书号:155066·1-47675 定价 39.00元

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国信息安全认证中心、公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人:甘杰夫、布宁、赵婷、陈晓桦、张笑笑、段静辉、吴迪。

信息安全技术　网站数据恢复产品技术要求与测试评价方法

1　范围

本标准规定了适用于互联网网站数据恢复产品技术要求与测试评价方法。

本标准适用于对网站数据恢复产品的研制、生产、测试和评价。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 5271.8—2001　信息技术　词汇　第8部分：安全

GB/T 18336.1—2008　信息技术　安全技术　信息技术安全性评估准则　第1部分：简介和一般模型

GB/Z 20986—2007　信息安全技术　信息安全事件分类分级指南

3　术语和定义

GB/T 5271.8—2001和GB/T 18336.1—2008界定的以及下列术语和定义适用于本文件。

3.1

网站数据　website data

与网站发布的内容相关的数据，包括静态网页文件、动态脚本文件、网页目录和网站数据库。

3.2

网站数据恢复　website data recovery

对遭受非授权更改的受保护的网站数据及时进行恢复的过程。

3.3

网站数据恢复产品　website data recovery product

用以实现网站数据恢复的软件或软硬件组合。

3.4

授权管理员　authorized administrator

具有使用网站数据恢复产品管理功能权限的管理员。

3.5

网站备份数据　backup for website

得到授权管理员认可的网站数据副本。

3.6

静态网页　static web page

当从WEB服务器下载到客户端时，其内容(正文、图像、表中的数据等)不会因访问对象或下载请求的不同而发生变化的网页。

3.7

动态网页　dynamic web page

当从 WEB 服务器下载到客户端时，其内容（正文、图像、表中的数据等）可根据访问对象或下载请求的不同而发生变化的网页。动态网页内容可由 WEB 服务器端脚本语言（如：PHP，Perl，ASP，ASP. NET，JSP 等）根据提交条件或状态生成。

3.8

动态脚本　dynamic script

一组脚本语言代码，用以支持生成动态网页。

3.9

完全备份　full backup

备份所有指定的数据对象的过程，不论这些数据自上次备份后是否被更改。完全备份是增量备份的基础。

3.10

增量备份　incremental backup

仅对自上次备份后更改过的数据对象进行备份的备份方式。

4　网站数据恢复产品等级划分

根据安全功能要求的不同，将网站数据恢复产品划分为两个等级：基本级和增强级。产品等级划分如表 1 所示。

第 5 章、第 6 章两章对每一等级的具体要求分别进行描述。其中“**加粗宋体字**”表示所描述的要求仅适用于增强级产品。

表 1　网站数据恢复产品等级划分表

技术要求			基本级	增强级
安全功能要求	网站数据监测功能	静态网页文件监测功能	*	*
		动态脚本文件监测功能		*
		网页目录监测功能	*	*
		网站数据库监测功能		*
	报警功能	实时报警事件	*	**
		报警方式	*	*
	网站数据自动恢复功能	静态网页文件自动恢复功能	*	*
		动态脚本文件自动恢复功能		*
		网页目录自动恢复功能	*	*
		网站数据库手动或自动恢复功能		*
	网站数据备份	网站数据备份初始化	*	*
		网站数据备份功能	*	*
		网站数据备份方式		*
	网站数据合法更新		*	**

表 1（续）

技术要求			基本级	增强级
安全功能要求	管理控制功能	监控对象管理	*	**
		远程管理		*
		管理界面友好性	*	*
		与网站发布系统的兼容性	*	*
		策略定制	*	*
		策略管理	*	*
	权限管理功能		*	*
	身份鉴别	身份鉴别	*	*
		鉴别失败处理	*	*
	审计功能	可审计事件	*	**
		审计数据内容	*	**
		审计迹管理	*	*
		内容可读性	*	*
		审计记录查询	*	*
	用户数据保护	管理信息传输安全	*	*
		备份数据的安全存储	*	*
		备份数据的安全传输	*	*
	程序数据保护	自身进程、服务保护	*	*
		程序文件保护	*	**
	抵御已知攻击	抵御木马、病毒的攻击	*	*
		抵御对网站数据库的攻击		*
安全保证要求	配置管理			*
	交付和运行		*	*
	开发			*
	指导性文档		*	*
	生命周期支持			*
	测试		*	**
	脆弱性评定			*

注：在表中，“空”表示产品不具备该项技术要求。“*”和“**”表示产品应具备该项技术要求。“**”相对于“*”，表示增强级产品相对于基本级产品在该项技术要求上进行了增强。

5 技术要求

5.1 基本级产品要求

5.1.1 安全功能要求

5.1.1.1 网站数据监测功能

5.1.1.1.1 静态网页文件监测功能

产品应监测受保护静态网页文件，并能发现对其进行的非授权更改，即：

a) 静态网页文件非授权增加的监控与审计；

b) 静态网页文件非授权删除的监控与审计；

c) 静态网页文件其他非授权修改(包括文件内容或属性修改、重命名、移动等)的监控与审计。

注：文件属性应至少包括文件创建及最后访问时间、文件大小和文件系统权限。下文中涉及文件属性的要求同此。

5.1.1.1.2 网页目录监测功能

产品应监测受保护网页目录，并能发现对其进行的非授权更改，即：

a) 网页目录非授权增加的监控与审计；

b) 网页目录非授权删除的监控与审计；

c) 网页目录其他非授权修改(包括目录属性修改、重命名、移动等)的监控与审计。

注：目录属性应至少包括目录创建及最后访问时间和文件系统权限。下文中涉及目录属性的要求同此。

5.1.1.2 报警功能

5.1.1.2.1 实时报警事件

产品应对以下事件进行实时报警：

a) 受保护静态网页文件、受保护网页目录被非授权增、删、改；

b) 实现网站数据监测功能(5.1.1.1)的监控保护程序的异常关闭。

5.1.1.2.2 报警方式

产品应提供适当的报警方式。如：E_mail 报警、声音或屏幕提示等报警方式。

5.1.1.3 网站数据自动恢复功能

5.1.1.3.1 静态网页文件自动恢复功能

产品应使用备份文件自动恢复遭受非授权更改的受保护静态网页文件，即：

a) 静态网页文件非授权增加的恢复；

b) 静态网页文件非授权删除的恢复；

c) 静态网页文件其他非授权修改(包括文件内容或属性修改、重命名、移动等)的恢复。

5.1.1.3.2 网页目录自动恢复功能

产品应使用备份目录自动恢复遭受非授权更改的受保护网页目录，即：

a) 网页目录非授权增加的恢复；

b) 网页目录非授权删除的恢复；

c) 网页目录其他非授权修改(包括目录属性修改、重命名、移动等)的恢复。

5.1.1.4 网站数据备份

5.1.1.4.1 网站数据备份初始化

产品在初次安装后应采取一定措施确保被监控的网站数据与网站备份数据一致,并保证网站备份数据的正确性和可用性。

5.1.1.4.2 网站数据备份功能

产品应实现对网站数据进行备份的功能,并保证备份的及时性。备份功能的实现可以采用完全备份或增量备份的方式进行。

5.1.1.5 网站数据合法更新

产品应提供或支持网站数据合法更新功能。该功能可以采用自动更新或手动更新的方式实现。手动更新时,产品应确保只有经授权的用户能够对网站数据(包括静态网页文件、网页目录)进行更新。自动更新时,产品应能够及时发现备份数据的变化,并自动同步该数据到 WEB 服务器,从而保证备份数据与被监控网站数据的一致性。

5.1.1.6 管理控制功能

5.1.1.6.1 监控对象管理

产品应能增加或撤消被监控的目录或文件。

5.1.1.6.2 管理界面友好性

产品应提供友好的管理界面,以便于对系统进行管理。

5.1.1.6.3 与网站发布系统的兼容性

产品应至少支持一种网站发布系统。安装产品后,产品及网站发布系统均能稳定运行。

5.1.1.6.4 策略定制

产品应支持对网站数据备份、网站数据合法更新、网站数据监测、网站数据恢复和事件报警方式等制定策略,或提供缺省配置策略。

5.1.1.6.5 策略管理

产品应支持对已配置的策略进行添加、删除、修改、分发、导入、导出等操作。

5.1.1.7 权限管理功能

产品应区分不同的用户角色,至少提供授权管理员和普通用户两种角色。

5.1.1.8 身份鉴别

5.1.1.8.1 身份鉴别

产品应对登录系统的用户至少采用一种身份鉴别方式进行身份鉴别,且身份鉴别功能应独立于操作系统自身的身份鉴别功能。

5.1.1.8.2 鉴别失败处理

产品应为登录系统的用户设定一个可修改的鉴别尝试阈值，当鉴别失败尝试超过阈值，系统应终止其与系统之间的会话过程。

5.1.1.9 审计功能

5.1.1.9.1 可审计事件

产品应对以下事件进行审计：

a) 受保护静态网页文件、受保护网页目录的增、删、改、恢复和合法更新；
b) 实现网站数据监测功能(5.1.1.1)的监控保护服务的开启和关闭；
c) 任何对鉴别机制的使用；
d) 对备份或恢复安全策略进行更改的操作；
e) 因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止；
f) 对管理角色进行增加、删除和属性修改的操作。

5.1.1.9.2 审计数据内容

审计数据中至少应包括事件发生的日期和时间、事件类型、主体身份等内容。日期应包含年、月、日，时间应包括时、分、秒。事件类型定义应遵照 GB/Z 20986—2007 的规定，并可根据事件的具体性质扩展相应子类，例如当发生网页文件被非授权删除的安全事件，其事件类型应为 GB/Z 20986—2007 中的 4.2.3 a)类型，并可扩展子类“网页文件被非授权删除”。若事件为 5.1.1.9.1 a)，则应指出受破坏静态网页文件、网页目录的位置和名称。

5.1.1.9.3 审计迹管理

授权管理员或其他获得授权的用户能存档、删除和清空审计记录。

5.1.1.9.4 内容可读性

审计记录内容应为中文，并应使存储于永久性审计记录中的所有审计数据为人所理解，不应有歧义。

5.1.1.9.5 审计记录查询

产品应能按条件或条件组合对审计记录进行查询。例如，按时间、事件类型、用户账户等条件进行查询。

5.1.1.10 用户数据保护

5.1.1.10.1 管理信息传输安全

若提供远程管理功能，应采取安全措施对传输的远程管理信息(例如，登录信息和会话信息)进行保护，如加密或使用专用信道等。

5.1.1.10.2 备份数据的安全存储

若需访问备份数据，应进行身份鉴别，以保证所有访问备份数据的操作均得到了正确的授权。

5.1.1.10.2.1 备份数据的安全传输

当通过网络进行网站数据备份或恢复时，应采取安全措施保证被传输数据的完整性。

5.1.1.11 程序数据保护

5.1.1.11.1 自身进程、服务保护

产品应具备防止非授权终止自身运行的措施。

5.1.1.11.2 程序文件保护

产品应采取保护措施，以保证部署在 WEB 服务器上的主要程序文件（如执行文件、日志库文件等）不被非授权删除或修改。

5.1.1.12 抵御已知攻击

5.1.1.12.1 抵御木马、病毒的攻击

产品应采取有效措施来抵御针对网站数据的木马、病毒等攻击手段，保证产品正常运行。

5.1.2 安全保证要求

5.1.2.1 交付和运行

5.1.2.1.1 交付

a) 开发者应使用交付程序给用户交付产品或其部分；
b) 开发者应采用文档的形式描述交付程序，该文档应描述在向用户方分发产品的各个版本时，用以维护其安全性所必需的所有程序。

5.1.2.1.2 安装、生成和启动

开发者应提供文档描述产品安全地安装、生成和启动必需的所有步骤。

5.1.2.2 指导性文档

5.1.2.2.1 管理员指南

a) 开发者应提供针对系统管理员的管理员指南。该指南应说明以下内容：
   1) 管理员可使用的管理功能和接口；
   2) 如何以安全的方式管理产品；
   3) 一些关于安全处理环境中应被控制的功能和特权的警示信息；
   4) 所有关于与产品安全运行有关用户行为的假设；
   5) 所有受管理员控制的安全参数，适当时应指明安全值；
   6) 每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制实体的安全特性；
   7) 所有与管理员有关的 IT 环境安全要求。
b) 管理员指南应与供评估的所有其他文档保持一致。

5.1.2.2.2 用户指南

a) 开发者应提供用户指南。该指南应说明以下内容：

1) 产品的非管理员用户可使用的功能和接口；
2) 产品所提供的用户可访问安全功能的使用；
3) 一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；
4) 产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；
5) 所有与用户有关的 IT 环境安全要求。

b) 用户指南应与供评估的所有其他文档保持一致。

5.1.2.3 测试

5.1.2.3.1 测试覆盖

开发者应提供测试覆盖的证据。测试覆盖的证据应说明测试文档中所标识的测试与功能规范中所描述的安全功能之间的对应性。

5.1.2.3.2 功能测试

a) 开发者应测试安全功能，并文档化测试结果。
b) 开发者应提供测试文档，测试文档应包括测试计划、测试程序描述、预期测试结果和实际测试结果。
c) 测试计划应标识要测试的安全功能和描述要执行的测试目标。
d) 测试程序描述应标识要执行的测试，并描述每个安全功能的测试脚本。这些脚本应包括对于其他测试结果的任何顺序依赖性。
e) 预期的测试结果应指出测试成功执行后的预期输出。
f) 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定运转。

5.1.2.3.3 独立测试

a) 开发者应提供用于测试的产品，该产品应适合测试；
b) 开发者应提供一组相当的资源，用于开发者的产品安全功能测试。

5.2 增强级产品要求

5.2.1 安全功能要求

5.2.1.1 网站数据监测功能

5.2.1.1.1 静态网页文件监测功能

产品应监测受保护静态网页文件，并能发现对其进行的非授权更改，即：

a) 静态网页文件非授权增加的监控与审计；
b) 静态网页文件非授权删除的监控与审计；
c) 静态网页文件其他非授权修改(包括文件内容或属性修改、重命名、移动等)的监控与审计。

5.2.1.1.2 动态脚本文件监测功能

产品应监测受保护动态脚本文件，并能发现对其进行的非授权更改，即：

a) 动态脚本文件非授权增加的监控与审计；
b) 动态脚本文件非授权删除的监控与审计；
c) 动态脚本文件其他非授权修改(包括文件内容或属性修改、重命名、移动等)的监控与审计。

5.2.1.1.3 网页目录监测功能

产品应监测受保护网页目录，并能发现对其进行的非授权更改，即：

a) 网页目录非授权增加的监控与审计；

b) 网页目录非授权删除的监控与审计；

c) 网页目录其他非授权修改(包括目录属性修改、重命名、移动等)的监控与审计。

5.2.1.1.4 网站数据库监测功能

产品应监测产品适用的受保护网站数据库，并能发现对其进行的非授权操作，包括：非授权登录尝试及增、删、改操作。

5.2.1.2 报警功能

5.2.1.2.1 实时报警事件

产品应对以下事件进行实时报警：

a) 受保护静态网页文件、**受保护动态脚本文件**、受保护网页目录被非授权增、删、改及**受保护网站数据库被非授权操作**；

b) **实现网站数据监测功能(5.1.1.1)的监控保护程序的异常关闭。**

5.2.1.2.2 报警方式

产品应提供适当的报警方式。如：E_mail 报警、声音或屏幕提示等报警方式。

5.2.1.3 网站数据自动恢复功能

5.2.1.3.1 静态网页文件自动恢复功能

产品应使用备份文件自动恢复遭受非授权更改的受保护静态网页文件，即：

a) 静态网页文件非授权增加的恢复；

b) 静态网页文件非授权删除的恢复；

c) 静态网页文件其他非授权修改(包括文件内容或属性修改、重命名、移动等)的恢复。

5.2.1.3.2 动态脚本文件自动恢复功能

产品应使用备份文件自动恢复遭受非授权更改的受保护动态脚本文件，即：

a) **动态脚本文件非授权增加的恢复；**

b) **动态脚本文件非授权删除的恢复；**

c) **动态脚本文件其他非授权修改(包括文件内容或属性修改、重命名、移动等)的恢复。**

5.2.1.3.3 网页目录自动恢复功能

产品应使用备份目录自动恢复遭受非授权更改的受保护网页目录，即：

a) 网页目录非授权增加的恢复；

b) 网页目录非授权删除的恢复；

c) 网页目录其他非授权修改(包括目录属性修改、重命名、移动等)的恢复。

5.2.1.3.4 网站数据库手动或自动恢复功能

产品应使用备份数据手动或自动恢复因非授权操作而改变的产品适用的数据库数据。

5.2.1.4 网站数据备份

5.2.1.4.1 网站数据备份初始化

产品在初次安装后应采取一定措施确保被监控的网站数据与网站备份数据一致，并保证网站备份数据的正确性和可用性。

5.2.1.4.2 网站数据备份功能

产品应实现对网站数据进行备份的功能，并保证备份的及时性。备份功能的实现可以采用完全备份或增量备份的方式进行。

5.2.1.4.3 网站数据备份方式

备份方式应支持手动备份和自动备份，自动备份应具备一定的实时性。

5.2.1.5 网站数据合法更新

产品应提供或支持网站数据合法更新功能。该功能可以采用自动更新或手动更新的方式实现。手动更新时，产品应确保只有经授权的用户能够对网站数据（包括静态网页文件、**动态脚本文件**、网页目录和**网站数据库**）进行更新。自动更新时，产品应能够及时发现备份数据的变化，并自动同步**该数据**到WEB服务器，从而保证备份数据与被监控网站数据的一致性。

5.2.1.6 管理控制功能

5.2.1.6.1 监控对象管理

产品应能增加或撤消被监控的目录、文件或**产品适用的网站数据库**。

5.2.1.6.2 远程管理

产品应提供远程管理功能，用户可通过远程方式进行管理。

5.2.1.6.3 管理界面友好性

产品应提供友好的管理界面，以便于对系统进行管理。

5.2.1.6.4 与网站发布系统的兼容性

产品应至少支持一种网站发布系统。安装产品后，产品及网站发布系统均能稳定运行。

5.2.1.6.5 策略定制

产品应支持对网站数据备份、网站数据合法更新、网站数据监测、网站数据恢复和事件报警方式等制定策略，或提供缺省配置策略。

5.2.1.6.6 策略管理

产品应支持对已配置的策略进行添加、删除、修改、分发、导入、导出等操作。

5.2.1.7 权限管理功能

产品应区分不同的用户角色，至少提供授权管理员和普通用户两种角色。

5.2.1.8 身份鉴别

5.2.1.8.1 身份鉴别

产品应对登录系统的用户至少采用一种身份鉴别方式进行身份鉴别，且身份鉴别功能应独立于操作系统自身的身份鉴别功能。

5.2.1.8.2 鉴别失败处理

产品应为登录系统的用户设定一个可修改的鉴别尝试阈值，当鉴别失败尝试超过阈值，系统应终止其与系统之间的会话过程。

5.2.1.9 审计功能

5.2.1.9.1 可审计事件

产品应对以下事件进行审计：

a) 受保护静态网页文件、**受保护动态脚本文件**、受保护网页目录的增、删、改、恢复和合法更新及**受保护数据库非授权操作和恢复**；

b) **实现网站数据监测功能(5.1.1.1)的监控保护服务的开启和关闭**；

c) 任何对鉴别机制的使用；

d) 对备份或恢复安全策略进行更改的操作；

e) **读取、修改、破坏审计迹数据的尝试**；

f) 因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止；

g) 对管理角色进行增加、删除和属性修改的操作；

h) **对其他安全功能配置参数的修改(设置和更新)，无论成功与否。**

5.2.1.9.2 审计数据内容

审计数据中至少应包括事件发生的日期和时间、事件类型、主体身份等内容。日期应包含年、月、日，时间应包括时、分、秒。事件类型定义应遵照 GB/Z 20986—2007 的规定，并可根据事件的具体性质扩展相应子类，例如当发生网页文件被非授权删除的安全事件，其事件类型应为 GB/Z 20986—2007 中的 4.2.3 a)类型，并可扩展子类“网页文件被非授权删除”。若事件为 5.2.1.9.1 a)，则应指出受破坏静态网页文件、**动态脚本文件**、网页目录或**网站数据库文件**的位置和名称。

5.2.1.9.3 审计迹管理

授权管理员或其他获得授权的用户能存档、删除和清空审计记录。

5.2.1.9.4 内容可读性

审计记录内容应为中文，并应使存储于永久性审计记录中的所有审计数据为人所理解，不应有歧义。

5.2.1.9.5 审计记录查询

产品应能按条件或条件组合对审计记录进行查询。例如，按时间、事件类型、用户账户等条件进行查询。

5.2.1.10 用户数据保护

5.2.1.10.1 管理信息传输安全

若提供远程管理功能，应采取安全措施对传输的远程管理信息（例如，登录信息和会话信息）进行保护，如加密或使用专用信道等。

5.2.1.10.2 备份数据的安全存储

若需访问备份数据，应进行身份鉴别，以保证所有访问备份数据的操作均得到了正确的授权。

5.2.1.10.3 备份数据的安全传输

当通过网络进行网站数据备份或恢复时，应采取安全措施保证被传输数据的完整性。

5.2.1.11 程序数据保护

5.2.1.11.1 自身进程、服务保护

产品应具备防止非授权终止自身运行的措施。

5.2.1.11.2 程序文件保护

产品应采取保护措施，以保证产品的主要程序文件（如执行文件、日志库文件等）不被非授权删除或修改。

5.2.1.12 抵御已知攻击

5.2.1.12.1 抵御木马、病毒的攻击

产品应采取有效措施来抵御针对网站数据的木马、病毒等攻击手段，保证产品正常运行。

5.2.1.12.2 抵御对网站数据库的攻击

产品应采取有效措施来阻止针对网站数据库的攻击，如针对动态网页的 SQL 注入式攻击。

5.2.2 安全保证要求

5.2.2.1 配置管理

5.2.2.1.1 配置管理能力

a) 开发者应为产品提供一个参照号，并在产品上进行标记，该参照号对产品的每一个版本应是唯一的；
b) 开发者应使用一个配置管理系统。配置管理系统应唯一标识产品所包含的所有配置项，且应提供措施使得只能对配置项进行授权改变；
c) 开发者应提供配置管理文档。配置管理文档应描述用于唯一标识产品所包含配置项的方法，并应提供所有配置项都已经和正在配置管理系统下有效地进行维护的证据。配置管理文档应包括一个配置清单和一个配置管理计划。配置清单应唯一标识组成产品的所有配置项，并应描述组成产品的配置项。配置管理计划应描述配置管理系统是如何使用的，且应提供证实配置管理系统的运行与配置管理计划是一致的证据。

5.2.2.1.2 配置管理范围

开发者应提供一个产品配置项列表。配置项列表应包括：实现表示和安全目标中其他保证组件所要求的评估证据。

5.2.2.2 交付和运行

5.2.2.2.1 交付

a) 开发者应使用交付程序给用户交付产品或其部分；
b) 开发者应采用文档的形式描述交付程序，该文档应描述在向用户方分发产品的各个版本时，用以维护其安全性所必需的所有程序。

5.2.2.2.2 安装、生成和启动

开发者应提供文档描述产品安全地安装、生成和启动必需的所有步骤。

5.2.2.3 开发

5.2.2.3.1 功能规范

开发者应当提供功能规范的设计文档，该文档应满足如下要求：
a) 对产品安全功能及其外部接口进行非形式化描述；
b) 保证其内在一致性；
c) 描述所有外部安全功能接口的用途与使用方法，适当时提供效果、例外情况和出错信息的细节；
d) 完备地表示产品安全功能。

5.2.2.3.2 高层设计

开发者应当提供产品安全功能的高层设计文档，该文档应满足如下要求：
a) 以非形式化方式表述，并且是内在一致的；
b) 按照子系统来描述产品安全功能的结构；
c) 描述每个产品安全功能子系统所提供的安全功能性；
d) 标识产品安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制提供功能的一个表示；
e) 标识产品安全功能子系统的所有接口；
f) 标识产品安全功能子系统的哪些接口是外部可见的；
g) 描述产品安全功能子系统所有接口的用途与使用方法，适当时提供效果、例外情况和出错消息的细节；
h) 把产品分成安全策略实施和其他子系统来描述。

5.2.2.3.3 表示对应性

a) 开发者应提供一个所提供产品安全功能表示的所有相邻对之间对应性的分析；
b) 对于所提供产品安全功能表示的每个相邻对，分析应证实，较为抽象的产品安全功能表示的所有相关安全功能都在较不抽象的安全功能表示中得到正确且完备的细化。

5.2.2.4 指导性文档

5.2.2.4.1 管理员指南

a) 开发者应提供针对系统管理员的管理员指南。该指南应说明以下内容：
   1) 管理员可使用的管理功能和接口；
   2) 如何以安全的方式管理产品；
   3) 一些关于安全处理环境中应被控制的功能和特权的警示信息；
   4) 所有关于与产品安全运行有关用户行为的假设；
   5) 所有受管理员控制的安全参数，适当时应指明安全值；
   6) 每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制实体的安全特性；
   7) 所有与管理员有关的 IT 环境安全要求。
b) 管理员指南应与供评估的所有其他文档保持一致。

5.2.2.4.2 用户指南

a) 开发者应提供用户指南。该指南应说明以下内容：
   1) 产品的非管理员用户可使用的功能和接口；
   2) 产品所提供的用户可访问安全功能的使用；
   3) 一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；
   4) 产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；
   5) 所有与用户有关的 IT 环境安全要求。
b) 用户指南应与供评估的所有其他文档保持一致。

5.2.2.5 生命周期支持

5.2.2.5.1 开发安全

开发者应提供开发安全文档，该文档应满足如下要求：

a) **描述在产品的开发环境中，保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施；**
b) **提供在产品的开发和维护过程中执行安全措施的证据。**

5.2.2.6 测试

5.2.2.6.1 测试覆盖

开发者应提供测试覆盖的一个分析，该分析应满足如下要求：

a) 证实测试文档中所标识的测试和功能规范中所描述的安全功能之间的对应性；
b) 证实功能规范中所描述安全功能和测试文档所标识的测试之间的对应性是完备的。

5.2.2.6.2 测试深度

开发者应提供测试深度的分析，深度分析应证实测试文档中所标识的测试足以证实该安全功能是依照其高层设计运行的。

5.2.2.6.3 功能测试

a) 开发者应测试安全功能，并文档化测试结果。
b) 开发者应提供测试文档，测试文档应包括测试计划、测试程序描述、预期测试结果和实际测试结果。
c) 测试计划应标识要测试的安全功能和描述要执行的测试目标。
d) 测试程序描述应标识要执行的测试，并描述每个安全功能的测试脚本。这些脚本应包括对于其他测试结果的任何顺序依赖性。
e) 预期的测试结果应指出测试成功执行后的预期输出。
f) 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定运转。

5.2.2.6.4 独立测试

a) 开发者应提供用于测试的产品，该产品应适合测试；
b) 开发者应提供一组相当的资源，用于开发者的产品安全功能测试。

5.2.2.7 脆弱性评定

5.2.2.7.1 脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。该文档满足如下要求：
a) 描述为搜索用户能违反产品安全策略的明显方法而执行的产品可交付材料分析；
b) 描述对明显的脆弱性的处置；
c) 针对所有已标识的脆弱性，说明脆弱性不能在产品的预期使用环境中被利用。

5.2.2.7.2 误用

开发者应提供指导性文档，该文档应满足如下要求：
a) 标识产品所有可能的运行方式(包括失败和操作失误后的运行)，它们的后果以及对于保持安全运行的意义；
b) 是完备的、清晰的、一致的、合理的；
c) 列出关于预期使用环境的所有假设；
d) 列出对外部安全措施(包括外部程序的、物理的或人员的控制)的所有要求。

6 测评方法

测评方法包括针对基本级产品和增强级产品的安全功能要求测试和安全保证要求评估。有关性能指标和测试方法参见附录 A。

6.1 测试环境与工具

网站数据恢复产品测试的典型网络拓扑结构如图 1 所示(图中各服务器、模块等之间的关系参见附录 B)：

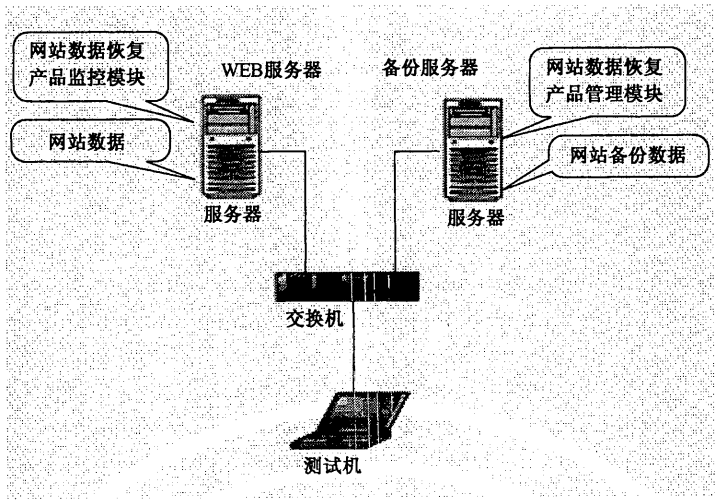

图 1　网站数据恢复产品测试典型网络拓扑图

6.2　基本级产品测试评价方法

6.2.1　安全功能要求测试

6.2.1.1　网站数据监测功能

6.2.1.1.1　静态网页文件监测功能

a)　测试方法：

1)　配置相关策略，指定需要监测的 WEB 服务器和相关目录、文件；

2)　尝试登录网页所在的 WEB 服务器，并分别进行以下操作：

——对受保护的静态网页文件进行非授权增加；

——对受保护的静态网页文件进行非授权删除；

——对受保护的静态网页文件进行非授权修改(包括文件属性修改、重命名、移动等)；

——对受保护的静态网页文件内容进行非授权添加、删除或修改。

3)　检查产品能否对非授权增加、删除和修改静态网页文件的事件进行实时报警，并且报警事件与实际情况相符。

b)　预期结果：

产品能对非授权增加、删除和修改静态网页文件的事件进行实时报警，并且报警事件与实际情况相符。

6.2.1.1.2　网页目录监测功能

a)　测试方法：

1)　配置相关策略，指定需要监测的 WEB 服务器和相关目录；

2)　尝试登录网页目录所在的 WEB 服务器，并分别进行以下操作：

——对受保护的网页目录进行非授权增加；

——对受保护的网页目录进行非授权删除；

——对受保护的网页目录进行非授权修改(包括目录属性修改、重命名、移动等)。

3)　检查产品能否对非授权增加、删除和修改网页目录的事件进行实时报警，并且报警事件与实际情况相符。

b)　预期结果：

产品能对非授权增加、删除和修改网页目录的事件进行实时报警，并且报警事件与实际情况相符。

6.2.1.2 报警功能

6.2.1.2.1 实时报警事件

a) 测试方法：

1) 尝试登录网页和网页目录所在的 WEB 服务器，并分别进行以下操作：

——对受保护的静态网页文件进行非授权增、删、改操作；

——对受保护的网页目录进行非授权增、删、改操作；

——尝试登录实现网站数据监测功能(5.1.1.1)的监控保护程序所在的服务器，并使用操作系统中的任务管理器关闭监控保护程序的进程和通过管理工具中“服务”关闭监控保护程序的服务。

2) 检查产品是否对以上由非授权操作引起的安全事件进行实时报警。

b) 预期结果：

产品对以上的所有事件都能进行实时报警。

6.2.1.2.2 报警方式

a) 测试方法：

1) 设置报警方式，并分别触发 5.1.1.2.1 中所列的事件；

2) 检查产品是否按照设定的方式进行了报警。

注：每种报警方式下，都应对 5.1.1.2.1 定义的所有事件进行测试。

b) 预期结果：

产品对 5.1.1.2.1 中的所有事件都能按照设定的方式进行报警。

6.2.1.3 网站数据自动恢复功能

6.2.1.3.1 静态网页文件自动恢复功能

a) 测试方法：

1) 配置相关策略，指定需要监测的 WEB 服务器和相关目录、文件；

2) 尝试登录网页所在的 WEB 服务器，并分别进行以下操作：

——对受保护的静态网页文件进行非授权增加；

——对受保护的静态网页文件进行非授权删除；

——对受保护的静态网页文件进行非授权修改(包括文件属性修改、重命名、移动等)；

——对受保护的静态网页文件的内容进行添加、删除或修改。

3) 检查产品能否使用备份文件自动恢复遭受非授权更改的静态网页文件。

b) 预期结果：

产品能自动删除非授权增加的静态网页文件，自动添加非授权删除的静态网页文件，自动恢复非授权修改的静态网页文件，自动恢复文件内容遭受非授权修改的静态网页文件。

6.2.1.3.2 网页目录自动恢复功能

a) 测试方法：

1) 配置相关策略，指定需要监测的 WEB 服务器和相关目录；

2) 尝试登录网页目录所在的 WEB 服务器，并分别进行以下操作：

——对受保护的网页目录进行非授权增加；

——对受保护的网页目录进行非授权删除；

——对受保护的网页目录进行非授权修改(包括目录属性修改、重命名、移动等)。

3) 检查产品能否使用备份目录自动恢复遭受非授权更改的网页目录。

b) 预期结果：

产品能自动删除非授权增加的网页目录，自动添加非授权删除的网页目录，自动恢复非授权修改的网页目录。

6.2.1.4 网站数据备份

6.2.1.4.1 网站数据备份初始化

a) 测试方法：

审查产品相关资料中是否存在对网站数据备份初始化的描述，并验证在初次安装产品后，系统是否采取措施确保被监控的网站数据与网站备份数据一致。

b) 预期结果：

产品在初次安装后，采取一定措施确保被监控的网站数据与网站备份数据一致。

6.2.1.4.2 网站数据备份功能

a) 测试方法：

1) 登录产品管理界面，验证产品是否能对网站数据合法更新进行及时备份；

2) 验证备份采用的是完全备份还是增量备份的手段实现。

b) 预期结果：

产品能对网站数据授权更新及时备份，并且备份功能实现满足要求。

6.2.1.5 网站数据合法更新

a) 测试方法：

登录产品管理界面，验证产品是否提供或支持自动或手动方式对网站数据进行合法更新的功能。同时，在手动更新时，验证只有经授权的用户能够对网站数据(包括静态网页文件、网页目录)进行更新；在自动更新时，验证产品能及时发现备份数据的变化，并自动同步该数据到WEB服务器。

b) 预期结果：

产品能提供网站数据合法更新功能，且该功能满足要求。

6.2.1.6 管理控制功能

6.2.1.6.1 监控对象管理

a) 测试方法：

1) 以普通用户身份登录产品管理界面，查看其监控内容，尝试增加或撤销本用户的被监控的目录或文件对象；

2) 以另一普通用户身份登录产品管理界面，查看其监控内容，确认管理界面未提供查看或修改其他用户的被监控目录或文件对象的功能；

3) 针对调整过的目录或文件引发报警事件，验证系统是否能进行报警。

b) 预期结果：

产品能实现此项功能。

6.2.1.6.2 管理界面友好性

a) 测试方法：

登录产品管理界面，进行各项管理操作，验证产品的管理界面是否友好。

b) 预期结果：

产品的管理界面布局应整齐、简洁，界面功能便于用户操作。

6.2.1.6.3 与网站发布系统的兼容性

a) 测试方法：

1) 把产品与几种网站发布系统分别进行配置；

2) 分别对产品和几种网站发布系统进行功能测试；

3) 验证产品和网站发布系统是否均能实现相应功能，并记录网站发布系统的型号。

b) 预期结果：

产品和至少一种网站发布系统均能实现相应功能。

6.2.1.6.4 策略定制

a) 测试方法：

1) 执行产品的各项待测策略定制功能；

2) 验证待测策略定制功能是否有效。

b) 预期结果：

产品能够有效地进行策略定制。

6.2.1.6.5 策略管理

a) 测试方法：

1) 执行产品的各项待测策略管理功能；

2) 验证待测策略管理功能是否有效。

b) 预期结果：

产品能够有效地进行策略管理。

6.2.1.7 权限管理功能

a) 测试方法：

创建多个用户，并为其设置不同权限。

b) 预期结果：

产品能区分不同用户角色，并至少提供授权管理员和普通用户两种角色。

6.2.1.8 身份鉴别

6.2.1.8.1 身份鉴别

a) 测试方法：

审查产品相关资料中对用户身份鉴别方式的描述，并且根据资料的介绍分别进行验证。

b) 预期结果：

产品对登录系统的用户至少采用一种身份鉴别方式，且身份鉴别功能独立于操作系统自身的身份鉴别功能。

6.2.1.8.2 鉴别失败处理

a) 测试方法：

1) 选取某个用户，设置其登录失败的尝试阈值；

2) 尝试以该用户名登录系统，并输入错误口令，直至超过设置的失败尝试阈值。

b) 预期结果：

产品支持用户登录的鉴别阈值设置，并在鉴别失败尝试超过设定阈值时终止其与系统之间的会话过程。

6.2.1.9 审计功能

6.2.1.9.1 可审计事件

a) 测试方法：

触发 5.1.1.9.1 中的所有事件，审查生成的审计记录。

b) 预期结果：

产品对 5.1.1.9.1 中的所有事件形成记录。

6.2.1.9.2 审计数据内容

a) 测试方法：

1) 分别触发 5.1.1.9.1 中的所有事件；

2) 审查产品的审计数据的内容是否包含了 5.1.1.9.2 中要求的内容。

b) 预期结果：

产品的审计信息至少包含了 5.1.1.9.2 中要求的内容。

6.2.1.9.3 审计迹管理

a) 测试方法：

1) 使用不同角色的用户登录产品，分别进行存档、删除和清空审计记录的操作；

2) 验证以上操作是否得到实施。

b) 预期结果：

仅获得授权的用户可以存档、删除和清空审计记录。

6.2.1.9.4 内容可读性

a) 测试方法：

查阅存储于永久性审计记录中的所有审计数据，验证数据的内容是否能理解且不存在歧义。

b) 预期结果：

存储于永久性审计记录中的审计数据内容能被操作者理解。

6.2.1.9.5 审计记录查询

a) 测试方法：

按条件或条件组合对审计记录进行查询。

b) 预期结果：

审计记录应能按条件或条件组合进行查询。

6.2.1.10 用户数据保护

6.2.1.10.1 管理信息传输安全

a) 测试方法：
若产品提供远程管理功能，验证该措施是否有效。
b) 预期结果：
若提供远程管理功能，产品对远程管理信息（例如，登录信息和会话信息）的传输采取安全措施进行保护。

6.2.1.10.2 备份数据的安全存储

a) 测试方法：
以不同的用户角色访问备份数据。
b) 预期结果：
仅得到授权的用户能访问备份数据。

6.2.1.10.3 备份数据的安全传输

a) 测试方法：
通过网络进行网站数据备份或恢复操作。
b) 预期结果：
产品应按照声明的方式保证被传输数据的完整性。

6.2.1.11 程序数据保护

6.2.1.11.1 自身进程、服务保护

a) 测试方法：
尝试非授权终止产品运行。
b) 预期结果：
产品具备防止非授权终止自身运行的措施。

6.2.1.11.2 程序文件保护

a) 测试方法：
尝试非授权删除或修改产品部署在 WEB 服务器上的主要程序文件（至少包括执行文件、日志库文件）。
b) 预期结果：
产品能阻止非授权的行为。

6.2.1.12 抵御已知攻击

6.2.1.12.1 抵御木马、病毒的攻击

a) 测试方法：
模拟针对网站数据的木马、病毒等攻击手段尝试破坏产品的正常运行。
b) 预期结果：
产品能抵御针对网站数据的木马、病毒等攻击手段，保证产品正常运行。

6.2.2 安全保证要求评估

6.2.2.1 交付和运行

6.2.2.1.1 交付

a) 评估方法：

1) 审查产品的交付文档，查看其是否具有安装文档、产品生成文档、指导用户进行产品运维的文档以及产品培训手册等文档；

2) 审查开发者是否提供了交付程序，该程序是否在文档中得到描述。

b) 预期结果：

交付中的全部要求都能得到满足。

6.2.2.1.2 安装、生成和启动

a) 评估方法：

审查开发者是否提供了文档描述了产品安全地安装、生成和启动所必要的步骤。

b) 预期结果：

安装、生成和启动中的全部要求都能得到满足。

6.2.2.2 指导性文档

6.2.2.2.1 管理员指南

a) 评估方法：

1) 审查产品的管理员指南，验证其是否：

——描述管理员可使用的管理功能和接口；

——描述如何以安全的方式管理产品；

——包含一些关于安全处理环境中应被控制的功能和特权的警示信息；

——描述所有关于与产品安全运行有关用户行为的假设；

——描述所有受管理员控制的安全参数，合适时指明安全值；

——描述每一种与需要执行的管理功能有关的安全相关事件，包括对改变安全功能所控制的实体的安全特性；

——描述所有与系统管理员有关的 IT 环境安全要求。

2) 审查产品的管理员指南，验证其是否与供评估的所有其他文档保持一致。

b) 预期结果：

管理员指南中的全部要求都能得到满足。

6.2.2.2.2 用户指南

a) 评估方法：

1) 审查产品的用户指南，验证其是否：

——描述非管理员用户可用的功能和接口；

——描述产品所提供的用户可以访问的安全功能的使用；

——包含一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；

——清晰地阐述产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；

——描述所有与用户有关的IT环境安全要求。

2) 审查产品的用户指南，验证其是否与评估而提供的其他所有文档保持一致。

b) 预期结果：

用户指南中的全部要求都能得到满足。

6.2.2.3 测试

6.2.2.3.1 测试覆盖

a) 评估方法：

审查开发者是否提供了测试覆盖的证据，并验证该证据是否说明了测试文档中所标识的测试和功能规范中所描述的安全功能之间是对应的。

b) 预期结果：

测试覆盖中的全部要求都能得到满足。

6.2.2.3.2 功能测试

a) 评估方法：

1) 审查测试文档是否包括测试计划、测试程序描述、预期测试结果和实际测试结果；

2) 审查测试计划是否标识了要测试的安全功能，描述了要执行的测试目标；

3) 审查测试程序描述是否标识了要执行的测试，并描述了每个安全功能的测试脚本，这些脚本包括对于其他测试结果的任意顺序依赖性；

4) 审查预期的测试结果是否与测试成功执行后的预期输出一致；

5) 审查文档中记录的预期测试结果和实际测试结果，确认每个被测试的安全性功能都按照规定运转。

b) 预期结果：

功能测试中的全部要求都能得到满足。

6.2.2.3.3 独立测试

a) 评估方法：

1) 检查开发者是否提供用于测试的产品，并且产品是否适合测试；

2) 检查开发者是否提供一组相当的资源，用于开发者的产品安全功能测试。

b) 预期结果：

独立测试中的全部要求都能得到满足。

6.3 增强级产品测试评价方法

6.3.1 安全功能要求测试

6.3.1.1 网站数据监测功能

6.3.1.1.1 静态网页文件监测功能

a) 测试方法：

1) 配置相关策略，指定需要监测的WEB服务器和相关目录、文件。

2) 尝试登录网页所在的WEB服务器，并分别进行以下操作：

——对受保护的静态网页文件进行非授权增加；

——对受保护的静态网页文件进行非授权删除；

——对受保护的静态网页文件进行非授权修改(包括文件属性修改、重命名、移动等);

——对受保护的静态网页文件内容进行非授权添加、删除或修改。

3) 检查产品能否对非授权增加、删除和修改静态网页文件的事件进行实时报警,并且报警事件与实际情况相符。

b) 预期结果:

产品能对非授权增加、删除和修改静态网页文件的事件进行实时报警,并且报警事件与实际情况相符。

6.3.1.1.2 动态脚本文件监测功能

a) 测试方法:

1) 配置相关策略,指定需要监测的 WEB 服务器和相关目录、文件。

2) 尝试登录动态脚本文件所在的 WEB 服务器,并分别进行以下操作:

——对受保护的动态脚本文件进行非授权增加;

——对受保护的动态脚本文件进行非授权删除;

——对受保护的动态脚本文件进行非授权修改(包括文件属性修改、重命名、移动等);

——对受保护的动态脚本文件的内容进行非授权添加、删除或修改。

3) 检查产品能否对非授权增加、删除和修改动态脚本文件的事件进行实时报警,并且报警事件与实际情况相符。

b) 预期结果:

产品能对非授权增加、删除和修改动态脚本文件的事件进行实时报警,并且报警事件与实际情况相符。

6.3.1.1.3 网页目录监测功能

a) 测试方法:

1) 配置相关策略,指定需要监测的 WEB 服务器和相关目录;

2) 尝试登录网页目录所在的 WEB 服务器,并分别进行以下操作:

——对受保护的网页目录进行非授权增加;

——对受保护的网页目录进行非授权删除;

——对受保护的网页目录进行非授权修改(包括目录属性修改、重命名、移动等)。

3) 检查产品能否对非授权增加、删除和修改网页目录的事件进行实时报警,并且报警事件与实际情况相符。

b) 预期结果:

产品能对非授权增加、删除和修改网页目录的事件进行实时报警,并且报警事件与实际情况相符。

6.3.1.1.4 网站数据库监测功能

a) 测试方法:

1) 在数据库服务器上安装产品适用的网站数据库;

2) 配置相关策略,指定需要监测的数据库服务器和相关目录、文件;

3) 尝试登录网站数据库服务器,并分别进行非授权的操作,如对受保护的网站数据库文件的内容进行添加、删除或修改等;

4) 检查产品能对这些非授权操作进行实时报警,并且报警事件与实际情况相符。

b) 预期结果：

产品能对非授权操作进行实时报警，并且报警事件与实际情况相符。

6.3.1.2 报警功能

6.3.1.2.1 实时报警事件

a) 测试方法：

1) 尝试登录网页和网页目录所在的 WEB 服务器，并分别进行以下操作：

——对受保护的静态网页文件进行非授权增、删、改操作；

——对受保护的动态脚本文件进行非授权增、删、改操作；

——对受保护的网页目录进行非授权增、删、改操作。

2) 尝试登录实现网站数据监测功能(5.1.1.1)的监控保护程序所在的服务器，并使用操作系统中的任务管理器关闭监控保护程序的进程和通过管理工具中“服务”关闭监控保护程序的服务；

3) **在数据库服务器上安装产品适用的网站数据库，尝试登录网站数据库所在数据库服务器，并对网站数据库进行非授权的操作，如对受保护的网站数据库文件的内容进行添加、删除或修改等；**

4) 检查产品是否对以上由非授权操作引起的安全事件进行实时报警。

b) 预期结果：

产品对以上的所有事件都能进行实时报警。

6.3.1.2.2 报警方式

a) 测试方法：

1) 设置报警方式，并分别触发 5.2.1.2.1 中所列的事件；

2) 检查产品是否按照设定的方式进行了报警。

注：每种报警方式下，都应对 5.2.1.2.1 定义的所有事件进行测试。

b) 预期结果：

产品对 5.2.1.2.1 中的所有事件都能按照设定的方式进行报警。

6.3.1.3 网站数据自动恢复功能

6.3.1.3.1 静态网页文件自动恢复功能

a) 测试方法：

1) 配置相关策略，指定需要监测的 WEB 服务器和相关目录、文件；

2) 尝试登录网页所在的 WEB 服务器，并分别进行以下操作：

——对受保护的静态网页文件进行非授权增加；

——对受保护的静态网页文件进行非授权删除；

——对受保护的静态网页文件进行非授权修改(包括文件属性修改、重命名、移动等)；

——对受保护的静态网页文件的内容进行添加、删除或修改。

3) 检查产品能否使用备份文件自动恢复遭受非授权更改的静态网页文件。

b) 预期结果：

产品能自动删除非授权增加的静态网页文件，自动添加非授权删除的静态网页文件，自动恢复非授权修改的静态网页文件，自动恢复文件内容遭受非授权修改的静态网页文件。

6.3.1.3.2 动态脚本文件自动恢复功能

a) 测试方法：

1) 配置相关策略，指定需要监测的 WEB 服务器和相关目录、文件；

2) 尝试登录动态脚本文件所在的 WEB 服务器，并分别进行以下操作：

——对受保护的动态脚本文件进行非授权增加；

——对受保护的动态脚本文件进行非授权删除；

——对受保护的动态脚本文件进行非授权修改(包括文件属性修改、重命名、移动等)；

——对受保护的动态脚本文件的内容进行添加、删除或修改。

3) 检查产品能否使用备份文件自动恢复遭受非授权更改的动态脚本文件。

b) 预期结果：

产品能自动删除非授权增加的动态脚本文件，自动添加非授权删除的动态脚本文件，自动恢复非授权修改的动态脚本文件，自动恢复文件内容遭受非授权修改的动态脚本文件。

6.3.1.3.3 网页目录自动恢复功能

a) 测试方法：

1) 配置相关策略，指定需要监测的 WEB 服务器和相关目录；

2) 尝试登录网页目录所在的 WEB 服务器，并分别进行以下操作：

——对受保护的网页目录进行非授权增加；

——对受保护的网页目录进行非授权删除；

——对受保护的网页目录进行非授权修改(包括目录属性修改、重命名、移动等)。

3) 检查产品能否使用备份目录自动恢复遭受非授权更改的网页目录。

b) 预期结果：

产品能自动删除非授权增加的网页目录，自动添加非授权删除的网页目录，自动恢复非授权修改的网页目录。

6.3.1.3.4 网站数据库手动或自动恢复功能

a) 测试方法：

1) 在数据库服务器上安装产品适用的网站数据库；

2) 配置相关策略，指定需要监测的数据库服务器和相关目录、文件；

3) 尝试登录网站数据库服务器，并进行非授权操作，如对受保护的网站数据库文件的内容进行添加、删除或修改等；

4) 检查产品能否使用备份数据以手动或自动的方式对因非授权操作而改变的产品适用的数据库数据进行恢复。

b) 预期结果：

产品能使用备份数据以手动或自动的方式恢复因非授权操作而改变的产品适用的数据库数据。

6.3.1.4 网站数据备份

6.3.1.4.1 网站数据备份初始化

a) 测试方法：

审查产品相关资料中是否存在对网站数据备份初始化的描述，并验证在初次安装产品后，系统

是否采取措施确保被监控的网站数据与网站备份数据一致。

b) 预期结果：

产品在初次安装后，采取一定措施确保被监控的网站数据与网站备份数据一致。

6.3.1.4.2 网站数据备份功能

a) 测试方法：

1) 登录产品管理界面，验证产品是否能对网站数据合法更新进行及时备份；

2) 验证备份是采用完全备份还是增量备份的手段实现。

b) 预期结果：

产品能对网站数据授权更新及时备份，并且备份功能实现满足要求。

6.3.1.4.3 网站数据备份方式

a) 测试方法：

登录产品管理界面，验证产品的备份方式是否支持手动备份和自动备份，自动备份是否具备一定的实时性。

b) 预期结果：

产品提供的网站数据备份方式支持手动备份和自动备份，自动备份具备一定的实时性。

6.3.1.5 网站数据合法更新

a) 测试方法：

登录产品管理界面，验证产品是否提供或支持自动或手动方式对网站数据进行合法更新的功能。同时，在手动更新时，验证只有经授权的用户能够对网站数据(包括静态网页文件、**动态脚本文件**、网页目录和**网站数据库**)进行更新；在自动更新时，验证产品能及时发现备份数据的变化，并自动同步该数据到 WEB 服务器。

b) 预期结果：

产品能提供网站数据合法更新功能，且该功能满足要求。

6.3.1.6 管理控制功能

6.3.1.6.1 监控对象管理

a) 测试方法：

1) 以普通用户身份登录产品管理界面，查看其监控内容，尝试增加或撤销本用户的被监控的目录或文件或**产品适用的数据库对象**；

2) 以另一普通用户身份登录产品管理界面，查看其监控内容，确认管理界面未提供查看或修改其他用户的被监控目录或文件或**产品适用的数据库对象的功能**；

3) 针对调整过的目录或文件或**产品适用的数据库**引发报警事件，验证系统是否能进行报警。

b) 预期结果：

产品能实现此项功能。

6.3.1.6.2 远程管理

a) 测试方法：

尝试通过网络远程登录产品管理入口，并进行各项管理操作。

b) 预期结果：

产品能通过远程正确地进行各项管理操作。

6.3.1.6.3 管理界面友好性

a) 测试方法：

登录产品管理界面，进行各项管理操作，验证产品的管理界面是否友好。

b) 预期结果：

产品的管理界面布局应整齐、简洁，界面功能便于用户操作。

6.3.1.6.4 与网站发布系统的兼容性

a) 测试方法：

1) 把产品与几种网站发布系统分别进行配置；

2) 分别对产品和几种网站发布系统的进行功能测试；

3) 验证产品和网站发布系统是否均能实现相应功能，并记录网站发布系统的型号。

b) 预期结果：

产品和至少一种网站发布系统均能实现相应功能。

6.3.1.6.5 策略定制

a) 测试方法：

1) 执行产品的各项待测策略定制功能；

2) 验证待测策略定制功能是否有效。

b) 预期结果：

产品能够有效地进行策略定制。

6.3.1.6.6 策略管理

a) 测试方法：

1) 执行产品的各项待测策略管理功能；

2) 验证待测策略管理功能是否有效。

b) 预期结果：

产品能够有效地进行策略管理。

6.3.1.7 权限管理功能

a) 测试方法：

创建多个用户，并为其设置不同权限。

b) 预期结果：

产品能区分不同用户角色，并至少提供授权管理员和普通用户两种角色。

6.3.1.8 身份鉴别

6.3.1.8.1 身份鉴别

a) 测试方法：

审查产品相关资料中对用户身份鉴别方式的描述，并且根据资料的介绍分别进行验证。

b) 预期结果：

产品对登录系统的用户至少采用一种身份鉴别方式，且身份鉴别功能独立于操作系统自身的

身份鉴别功能。

6.3.1.8.2 鉴别失败处理

a) 测试方法：

1) 选取某个用户，设置其登录失败的尝试阈值；

2) 尝试以该用户名登录系统，并输入错误口令，直至超过设置的失败尝试阈值。

b) 预期结果：

产品支持用户登录的鉴别阈值设置，并在鉴别失败尝试超过设定阈值时终止其与系统之间的会话过程。

6.3.1.9 审计功能

6.3.1.9.1 可审计事件

a) 测试方法：

触发 5.2.1.9.1 中的所有事件，审查生成的审计记录。

b) 预期结果：

产品对 5.2.1.9.1 中的所有事件形成记录。

6.3.1.9.2 审计数据内容

a) 测试方法：

1) **分别触发 5.2.1.9.1 中的所有事件；**

2) **审查产品的审计数据的内容是否包含了 5.2.1.9.2 中要求的内容。**

b) 预期结果：

产品的审计信息至少包含了 5.2.1.9.2 中要求的内容。

6.3.1.9.3 审计迹管理

a) 测试方法：

1) 使用不同角色的用户登录产品，分别进行存档、删除和清空审计记录的操作；

2) 验证以上操作是否得到实施。

b) 预期结果：

仅获得授权的用户可以存档、删除和清空审计记录。

6.3.1.9.4 内容可读性

a) 测试方法：

查阅存储于永久性审计记录中的所有审计数据，验证数据的内容是否能理解且不存在歧义。

b) 预期结果：

存储于永久性审计记录中的审计数据内容能被操作者理解。

6.3.1.9.5 审计记录查询

a) 测试方法：

按条件或条件组合对审计记录进行查询。

b) 预期结果：

审计记录应能按条件或条件组合进行查询。

6.3.1.10 用户数据保护

6.3.1.10.1 管理信息传输安全

a) 测试方法：
若产品提供远程管理功能，验证该措施是否有效。
b) 预期结果：
若提供远程管理功能，产品对远程管理信息（例如，登录信息和会话信息）的传输采取安全措施进行保护。

6.3.1.10.2 备份数据的安全存储

a) 测试方法：
以不同的用户角色访问备份数据。
b) 预期结果：
仅得到授权的用户能访问备份数据。

6.3.1.10.3 备份数据的安全传输

a) 测试方法：
通过网络进行网站数据备份或恢复操作。
b) 预期结果：
产品应按照声明的方式保证被传输数据的完整性。

6.3.1.11 程序数据保护

6.3.1.11.1 自身进程、服务保护

a) 测试方法：
尝试非授权终止产品运行。
b) 预期结果：
产品具备防止非授权终止自身运行的措施。

6.3.1.11.2 程序文件保护

a) 测试方法：
尝试非授权删除或修改产品主要程序文件（至少包括执行文件、日志库文件）。
b) 预期结果：
产品能阻止非授权的行为。

6.3.1.12 抵御已知攻击

6.3.1.12.1 抵御木马、病毒的攻击

a) 测试方法：
模拟针对网站数据的木马、病毒等攻击手段尝试破坏产品的正常运行。
b) 预期结果：
产品能抵御针对网站数据的木马、病毒等攻击手段，保证产品正常运行。

6.3.1.12.2 抵御对网站数据库的攻击

a) 测试方法：
模拟针对网站数据库的攻击。
b) 预期结果：
产品能阻止针对网站数据库的攻击。

6.3.2 安全保证要求评估

6.3.2.1 配置管理

6.3.2.1.1 配置管理能力

a) 评估方法：
1) 检查每个版本的产品是否具有唯一的参照号；
2) 检测产品提供的配置管理系统，验证其是否能唯一标识产品所包含的所有配置项，是否提供措施使得对配置项只能进行授权修改；
3) 审查产品的配置管理文档中是否包括了配置清单和配置计划，审查配置清单是否描述并唯一标识了组成产品的所有配置项，审查配置计划是否描述了配置管理系统使用方法以及配置管理系统的运作和配置管理计划是否相一致，审查配置管理文档是否描述用于唯一标识产品所包含配置项的方法，是否提供所有配置项都已经或正在配置管理系统下有效地进行维护的证据。
b) 预期结果：
配置管理能力中的全部要求都能得到满足。

6.3.2.1.2 配置管理范围

a) 评估方法：
审查开发者是否提供了产品配置项列表，且配置项列表包括：实现表示和安全目标中其他保证组件所要求的评估证据。
b) 预期结果：
配置管理范围中的全部要求都能得到满足。

6.3.2.2 交付和运行

6.3.2.2.1 交付

a) 评估方法：
1) 审查产品的交付文档，查看其是否具有安装文档、产品生成文档、指导用户进行产品运维的文档以及产品培训手册等文档；
2) 审查开发者是否提供了交付程序，该程序是否在文档中得到描述。
b) 预期结果：
交付中的全部要求都能得到满足。

6.3.2.2.2 安装、生成和启动

a) 评估方法：
审查开发者是否提供了文档描述了产品安全地安装、生成和启动所必要的步骤。

b) 预期结果：

安装、生成和启动中的全部要求都能得到满足。

6.3.2.3 开发

6.3.2.3.1 功能规范

a) 评估方法：

1) 审查产品的开发文档，查看是否具有功能规范设计文档；

2) 审查功能规范设计文档，确认其是否描述了产品的所有安全功能和外部接口，是否包括所有外部安全功能接口的使用方法和用途，是否是内在一致的，是否能完备地表示产品安全功能。

b) 预期结果：

功能规范中的全部要求都能得到满足。

6.3.2.3.2 高层设计

a) 评估方法：

1) 审查产品的开发文档，查看是否具有高层设计文档；

2) 审查高层设计文档，确认其是否按照子系统来描述产品安全功能的结构，是否描述了每个产品安全功能子系统所提供的安全功能性，是否标识了安全功能子系统的所有接口，是否标识了产品安全功能子系统的哪些接口是外部可见的，是否标识了产品安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制提供功能的一个表示，是否描述产品安全功能子系统所有接口的用途与使用方法，是否把产品分成安全策略实施和其他子系统来描述，是否以非形式化方式进行描述，是否是内在一致的。

b) 预期结果：

高层设计中的全部要求都能得到满足。

6.3.2.3.3 表示对应性

a) 评估方法：

审查对应性分析报告，确认是否论证了功能规范中所有的相关安全功能都在高层设计中得到正确且完备的细化。

b) 预期结果：

表示对应性中的全部要求都能得到满足。

6.3.2.4 指导性文档

6.3.2.4.1 管理员指南

a) 评估方法：

1) 审查产品的管理员指南，验证其是否：

——描述管理员可使用的管理功能和接口；

——描述如何以安全的方式管理产品；

——包含一些关于安全处理环境中应被控制的功能和特权的警示信息；

——描述所有关于与产品安全运行有关用户行为的假设；

——描述所有受管理员控制的安全参数，合适时指明安全值；

——描述每一种与需要执行的管理功能有关的安全相关事件，包括对改变安全功能所控制的实体的安全特性；

——描述所有与系统管理员有关的 IT 环境安全要求。

2) 审查产品的管理员指南，验证其是否与供评估的所有其他文档保持一致。

b) 预期结果：

管理员指南中的全部要求都能得到满足。

6.3.2.4.2 用户指南

a) 评估方法：

1) 审查产品的用户指南，验证其是否：

——描述非管理员用户可用的功能和接口；

——描述产品所提供的用户可以访问的安全功能的使用；

——包含一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；

——清晰地阐述产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；

——描述所有与用户有关的 IT 环境安全要求。

2) 审查产品的用户指南，验证其是否与评估而提供的其他所有文档保持一致。

b) 预期结果：

用户指南中的全部要求都能得到满足。

6.3.2.5 生命周期支持

6.3.2.5.1 开发安全

a) 评估方法：

1) **审查开发者是否提供了开发安全文档，验证开发文档是否描述了在产品的开发环境中，保护产品设计和实现的保密性和完整性在物理、程序、人员以及其他方面必要的安全措施；**

2) **审查开发安全文档是否提供了产品的开发和维护过程中执行安全措施的证据。**

b) 预期结果：

开发安全中的全部要求都能得到满足。

6.3.2.6 测试

6.3.2.6.1 测试覆盖

a) 评估方法：

审查开发者提供的测试覆盖**分析**，验证该**分析**是否**证实**了测试文档中所标识的测试和功能规范中所描述的安全功能是对应的，**验证功能规范中所描述安全功能和测试文档所标识的测试之间的对应性是否完备。**

b) 预期结果：

测试覆盖中的全部要求都能得到满足。

6.3.2.6.2 测试深度

a) 评估方法：

审查开发者是否提供了测试深度分析文档，验证测试文档中所标识的测试是否足以证明该安全功能是依照其高层设计运行的。

b) 预期结果：

测试深度中的全部要求都能得到满足。

6.3.2.6.3 功能测试

a) 评估方法：

1) 审查测试文档是否包括测试计划、测试程序描述、预期测试结果和实际测试结果；
2) 审查测试计划是否标识了要测试的安全功能，描述了要执行的测试目标；
3) 审查测试程序描述是否标识了要执行的测试，并描述了每个安全功能的测试脚本，这些脚本包括对于其他测试结果的任意顺序依赖性；
4) 审查预期的测试结果是否与测试成功执行后的预期输出一致；
5) 审查文档中记录的预期测试结果和实际测试结果，确认每个被测试的安全性功能都按照规定运转。

b) 预期结果：

功能测试中的全部要求都能得到满足。

6.3.2.6.4 独立测试

a) 评估方法：

1) 检查开发者是否提供用于测试的产品，并且产品是否适合测试；
2) 检查开发者是否提供一组相当的资源，用于开发者的产品安全功能测试。

b) 预期结果：

独立测试中的全部要求都能得到满足。

6.3.2.7 脆弱性评定

6.3.2.7.1 脆弱性分析

a) 评估方法：

1) **检查产品是否提供了脆弱性分析文档；**
2) **审查脆弱性文档是否描述为搜索用户能违反产品安全策略的明显方法而执行的产品可交付材料分析；**
3) **审查脆弱性文档，确认是否描述了明显的脆弱性的处置方法；**
4) **审查脆弱性文档，确认是否针对所有已标识的脆弱性，说明了脆弱性不能在产品的预期使用环境中被利用。**

b) 预期结果：

脆弱性分析中的全部要求都能得到满足。

6.3.2.7.2 误用

a) 评估方法：

审查开发者是否提供了指导性文档，该文档是否描述了产品所有可能的运行方式(包括失败和操作失误后的运行)、它们的后果以及对于保持安全运行的意义，是否列出关于预期使用环境的所有假设，是否列出外部安全措施(包括外部程序的、物理的或人员的控制)的所有要求，是否是完备的、清晰的、一致的、合理的。

b) 预期结果：

误用中的全部要求都能得到满足。

附 录 A
（资料性附录）
性能指标与测试

A.1 性能指标

A.1.1 监控响应时间

监控响应时间是指发现网站数据被非授权更改到对其进行报警所需的时间。该时间越短表示产品性能越好。

A.1.2 篡改恢复时间

篡改恢复时间是指发现网站数据被非授权更改到对其进行自动恢复所需的时间。该时间越短表示产品性能越好。

A.1.3 网络影响

安装产品后，产品不应对网站浏览产生太大影响，可以用安装产品前后网站的响应速度评价。

A.1.4 稳定性

安装产品后，产品以及相应的网站系统均能稳定运行。稳定性可用平均无故障率等指标进行评价。

A.2 性能测试

A.2.1 监控响应时间

a) 测试方法：
   1) 配置测试环境，使用第三方计时工具记录非授权用户删除网站数据的时间和产品报警的时间；
   2) 根据两个时间之差计算出监控响应时间。
b) 测试结果：
   根据实际测试情况，记录测试所用工具、参数以及测试结果。

A.2.2 篡改恢复时间

a) 测试方法：
   1) 配置测试环境，记录待修改文件的大小；
   2) 使用第三方计时工具记录网站数据被非授权更改到对其进行自动恢复所需的时间。
b) 测试结果：
   根据实际测试情况，记录测试所用工具、参数以及测试结果。

A.2.3 网络影响

a) 测试方法：
   配置测试环境，使用第三方计时工具记录网站在安装产品前后访问时间的变化，并记录该项测

试的参数。

b) 测试结果：

根据实际测试情况，记录测试所用工具、参数以及测试结果。

A.2.4 稳定性

a) 测试方法：

配置测试环境，并连续运行系统至少 7 天，在此期间可以触发一些事件使得产品进行相应的操作，检查产品在工作环境中是否能正常运行以及是否造成相应的网站系统崩溃或异常。

b) 测试结果：

根据实际测试情况，记录测试所用工具、参数以及测试结果。

附 录 B
（资料性附录）
网站数据恢复过程示例

网站恢复一般是在监测到网站数据内容被非授权更改后，及时产生报警，并进行准实时的自动恢复。网站恢复一般涉及3个环节：备份环节、监测环节和恢复环节。

B.1 备份环节

备份环节主要对网站数据进行备份，保存或更新网站备份数据。网站备份数据可以存放在WEB服务器或与WEB服务器相连的远程服务器。

B.2 监测环节

监测环节主要检查网站数据内容是否被非授权更改，并根据检查结果产生相应报警。

B.2.1 监测方式

监测操作可以在WEB服务器或与WEB服务器相连远程服务器上进行，采用定时检测方式、触发方式或其他方式。

B.2.1.1 定时检测方式

定时检测方式根据设定的时间定时读出要监控的网站数据（或其他能用以判断网站数据是否被更改的信息，例如，相应的文件属性等），将其与网站备份数据相比较，从而判断网站数据是否被更改。

为提高检测效率，可能将网站数据分为不同等级，对不同等级的网站数据设置不同的检测时间。例如，将高等级网站数据的检测时间间隔设得较短，以获得较好的实时性；而将等级较低的网站数据检测时间间隔设得较长，以减轻系统的负担。

B.2.1.2 触发方式

触发方式通过一些特定的事件来触发检测操作，而不是定时地、主动地对网站数据进行检测。这些特定事件可能是文件被访问、创建、修改或删除等。

例如，当用户访问某个网页的时候触发对该网页进行完整性检查。或利用一些特殊技术（例如，文件过滤驱动程序）捕获网站文件被访问、创建、修改或删除等事件，从而触发检测操作。

B.2.2 比较方式

在判断文件是否被修改时，往往采用将被保护的网站数据和网站备份数据进行比较的方式进行。

B.2.2.1 全文比较

这是最常用的比较方式，它能直接、准确地判断出该文件是否被修改。然而全文比较在文件较大较多时效率十分低下。

一些保护软件采用文件的属性如文件大小、创建修改时间等进行比较。这种方法虽然简单高效，但也有严重的缺陷：恶意入侵者可以通过精心构造，把替换文件的属性设置得和原文件完全相同，从而使被恶意更改的文件无法被检测出来。

B.2.2.2 函数比较

通过比较文件的 Hash 值(例如,MD5 算法)判断文件是否被修改。这种比较方式效率高,难以伪造,能比较精确地发现文件被篡改。

B.3 恢复环节

当监测到网站数据内容被非授权更改后启动恢复环节,使用网站备份数据替换被非授权更改的网站数据。

根据网站备份数据存放的位置不同,恢复操作可以分为本地或远程方式。

如果网站备份数据存放在 WEB 服务器,则需要拥有对被保护目录或文件的写权限。如果网站备份数据存放在与 WEB 服务器相连的远程服务器,则需要通过其他方式进行,例如,文件共享或 FTP 的方式,相应地,需要文件共享或 FTP 的账号,并且该账号拥有对被保护目录或文件的写权限。

GB/T 29766-2013

*
书号:155066 · 1-47675
定价: 39.00 元

打印日期:2013年10月15日 F009