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

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

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。

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。

目　次