ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37956—2019

信息安全技术
网站安全云防护平台技术要求

Information security technology—
Technology requirement for website security cloud protection platform

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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:国家工业信息安全发展研究中心、北京知道创宇信息技术有限公司、公安部第三研究所、中国信息安全研究院有限公司、网神信息技术(北京)股份有限公司、阿里云计算有限公司、杭州安恒信息技术股份有限公司、深信服科技股份有限公司。

本标准主要起草人:张格、于盟、张哲宇、赵光明、宋好好、尹丽波、何小龙、刘迎、左晓栋、顾健、杨晨、王朋涛、王枭卿、周俊、宋志明、陈雪秀、李鸿培、吴艳艳、唐旺、江浩、刘文胜、肖俊芳、李俊、郭娴、赵伟、周欣、刘伯仲、陈妍、陆臻、毛润华、张弛。

信息安全技术
网站安全云防护平台技术要求

1 范围

本标准规定了网站安全云防护平台的技术要求，包括平台功能要求和平台安全要求。

本标准适用于网站安全云防护平台的开发、运营及使用，为政府部门、企事业单位、社会团体等组织或个人选购网站安全云防护平台提供参考。

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 25069—2010 信息安全技术 术语

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32917—2016 信息安全技术 WEB应用防火墙安全技术要求与测试评价方法

3 术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

网站安全云防护平台 website security cloud protection platform

以云服务模式提供网站安全防护，运用集中管控、协同防御等方式，及时更新防护策略和规则，对网站访问请求和响应进行检测、分析、过滤的安全防护节点的集合。

3.2

网站安全云防护平台提供者 website security protection cloud platform providers

负责建立、运营网站安全云防护平台相关的基础设施、网络拓扑结构、防护功能组件等，在此平台上执行安全防护、保障网站安全的组织或机构。

3.3

网站安全云防护平台用户 website security cloud protection platform users

使用网站安全云防护平台的组织或个人。

3.4

平台用户网站数据 platform users website data

网站安全云防护平台用户的网站相关数据。

注：包括网站信息、原始访问流量、访问日志、操作日志、被攻击日志等。

3.5

网站运营者 website operators

负责网站后期运作、维护、经营的组织或个人。

4 缩略语

下列缩略语适用于本文件。

ACK:确认字符 (Acknowledgement)

API:应用程序编程接口(Application Programming Interface)

CC:挑战黑洞(Challenge Collapsar)

DNS:域名系统(Domain Name System)

HTTP:超文本传输协议(HyperText Transfer Protocol)

ICMP:网际控制报文协议(Internet Control Message Protocol)

IP:网际协议(Internet Protocol)

SYN:TCP 连接同步信号(Synchronous)

TCP:传输控制协议(Transport Control Protocol)

UDP:用户数据报协议(User Datagram Protocol)

URL:统一资源定位符(Uniform Resource Locator)

WEB:万维网(World Wide Web)

5 概述

网站安全云防护平台由相互联系、统一调度的安全防护节点组成,平台通过云服务模式,集中快速地部署、更新防护策略,对网站恶意请求进行过滤和清洗,提高网站安全防护能力。

网站安全云防护平台技术要求分为平台功能要求和平台安全要求两个方面,功能要求包括网站安全防护、网站合规性检查、资源管理、策略管理等;安全要求包括系统与通信保护、访问控制、配置管理、安全事件处置、平台容灾备份等。

根据防护网站所承载的业务和信息的敏感程度,网站安全云防护平台技术要求分为一般要求和增强要求。一般要求是网站安全云防护平台在开展网站安全防护业务应具备的基本功能及安全要求。增强要求是对一般要求的补充和强化。网站安全云防护平台用户可根据自身业务类型及承载信息的敏感程度选择相应安全要求的网站安全云防护平台,GB/T 31167—2014 中 6.3 和 6.4 给出了判断业务类型及承载信息的敏感程度的相应方法。

6 平台功能要求

6.1 网站安全防护

6.1.1 WEB 攻击防御

6.1.1.1 一般要求

应支持识别 WEB 攻击类型,阻断直接或间接的攻击行为,包括:

a) GB/T 32917—2016 中 4.1.1.2.2 要求的安全防护功能;

b) 暴力破解防护;

c) Webshell 识别和拦截;

d) 目录遍历防护;

e) Cookie 注入攻击防护;

f) 恶意代码执行防护。

6.1.1.2 增强要求

应具备其他 WEB 攻击防护功能。

6.1.2 DDoS 攻击防御

6.1.2.1 一般要求

应支持 DDoS 清洗，具备防御 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、HTTP Flood、DNS Flood、CC 攻击等拒绝服务类攻击的功能。

6.1.2.2 增强要求

无。

6.1.3 防护策略配置

6.1.3.1 一般要求

应满足以下要求：

a) 提供默认安全防护策略；
b) 提供检测、防护等策略模式；
c) 支持平台用户配置与选择防护策略。

6.1.3.2 增强要求

应支持平台用户查阅阻断的访问请求和对应的防护策略，反馈漏报及误报信息。

6.1.4 协同防御

6.1.4.1 一般要求

应满足以下要求：

a) 支持识别攻击常用域名、IP 地址等信息，记录并分析攻击者行为，在整个云防护范围内对恶意攻击者 IP 地址等进行阻断；
b) 对可信第三方提供的恶意攻击 IP 地址等信息，应支持识别、分析并在整个云防护范围内阻断。

6.1.4.2 增强要求

无。

6.1.5 内容安全

6.1.5.1 敏感信息过滤

6.1.5.1.1 一般要求

应支持自定义敏感词汇，对网站文字内容中出现的敏感词汇进行过滤。

6.1.5.1.2 增强要求

可支持对涉及敏感信息的图片等内容进行过滤。

6.1.5.2 错误页面处理

6.1.5.2.1 一般要求

应满足以下要求：

a) 支持对网站服务器返回的错误页面进行自定义，出错消息不能泄露与网站安全相关内容；

b) 支持仅向授权人员展示出错消息。

6.1.5.2.2 增强要求

无。

6.1.5.3 篡改应对

6.1.5.3.1 一般要求

应支持预定义时间内，提供平台用户指定的未篡改页面镜像，并在发现异常时告警的功能。

6.1.5.3.2 增强要求

应支持预定义时间内，自动监测发现页面篡改。

6.1.6 网站监测

6.1.6.1 一般要求

应满足以下要求：

a) 应支持网站可用性监测；

b) 应监测并记录网站被攻击情况，包括攻击类型、攻击时间等，在发现异常时向平台用户发出告警。

6.1.6.2 增强要求

无。

6.1.7 网站访问控制

6.1.7.1 一般要求

应满足以下要求：

a) 支持设置 IP 地址白名单或网站 URL 白名单，为网站访问者保留访问通道；

b) 支持设置 IP 地址黑名单，对列入 IP 地址黑名单的访问者进行阻断；

c) 支持在预定义时间段内，对网站的任何访问请求进行访问控制，设置为阻断/通过；

d) 支持预定义 URL 页面的访问请求设置为阻断/通过；

e) 以上访问控制策略的组合使用。

6.1.7.2 增强要求

无。

6.2 网站合规性检查

6.2.1 一般要求

应支持在网站接入前进行合规性检查，拒绝不合规如未备案网站的接入。

6.2.2 增强要求

应支持定期复查已接入网站合规性情况。

6.3 资源管理

6.3.1 资源运行监测

6.3.1.1 一般要求

应满足以下要求：

a) 支持对支撑平台运行的 DNS、带宽、防护节点等软硬件平台资源进行统一监测；
b) 支持对防护节点/主机的网络带宽、流量处理延时、主机系统负载、站点访问成功率等资源使用情况进行统一检测；
c) 支持及时发现资源使用异常并告警；
d) 支持对资源使用情况、平台承载业务量进行定期分析，评估当前业务、平台用户扩容及新用户接入的需求，并生成分析报告；
e) 应提供对资源使用记录的查询、统计及报表输出功能。

6.3.1.2 增强要求

无。

6.3.2 资源集中管控

6.3.2.1 一般要求

应满足以下要求：

a) 支持对支撑平台运行的 DNS、带宽、防护节点等平台资源的集中调配；
b) 支持依据防护节点/主机资源使用的分析结果对网站访问流量通过 DNS 在广域网或防护节点内部进行调配；
c) 支持对网站及用户配置信息、平台日志信息等资源集中分析和维护；
d) 支持平台资源集中调配在不间断服务情况下进行。

6.3.2.2 增强要求

无。

6.4 策略管理

6.4.1 策略集中管控

6.4.1.1 一般要求

应满足对网站防护策略进行集中维护和管理，支持策略配置的集中添加、修改、停用。

6.4.1.2 增强要求

无。

6.4.2 策略优化更新

6.4.2.1 一般要求

应满足以下要求：

a) 支持及时优化网站安全防护策略；
b) 支持对未知攻击手段及 WEB 安全漏洞的及时跟踪、发现、应对；
c) 支持在 WEB 安全漏洞通报后及时增加相应安全防护规则或更新安全防护策略。

6.4.2.2 增强要求

无。

6.5 统计分析

6.5.1 一般要求

应满足以下要求：

a) 支持对某一时间段内告警日志进行统计分析；
b) 支持对不同攻击类型事件数量进行统计分析；
c) 支持对攻击地理区域进行统计分析；
d) 支持对攻击源 IP 进行统计分析；
e) 以上数据统计的可视化图表，支持按照日、周和自定义时间等时间维度进行展示。

6.5.2 增强要求

无。

6.6 系统扩展

6.6.1 一般要求

无。

6.6.2 增强要求

应支持对外部系统提供各类 API 接口，包括日志接口，安全策略接口，报表接口等。

7 平台安全要求

7.1 系统与通信保护

7.1.1 一般要求

应满足 GB/T 31168—2014 中 6.2.1、6.6.1 和 6.11.1 的一般要求。

7.1.2 增强要求

应满足 GB/T 31168—2014 中 6.2.2[除 a)、g)外]、6.3.2 和 6.11.2 的增强要求。

7.2 访问控制

7.2.1 一般要求

应满足 GB/T 31168—2014 中 7.2.1、7.4.1、7.5.1、7.6.1、7.7.1、7.8.1、7.9.1、7.11.1、7.12.1 和 7.13.1 的一般要求。

7.2.2 增强要求

应满足 GB/T 31168—2014 中 7.2.2、7.3.2、7.8.2 和 7.11.2 的增强要求。

7.3 配置管理

7.3.1 一般要求

应满足 GB/T 31168—2014 中 8.3.1、8.4.1 和 8.6.1 的一般要求。

7.3.2 增强要求

应满足 GB/T 31168—2014 中 8.3.2、8.4.2 和 8.6.2 的增强要求。

7.4 安全事件处置

7.4.1 一般要求

应满足以下要求：

a) 支持及时发布影响平台自身及平台用户的安全事件风险提示和预警；
b) 支持在发生重大及以上安全事件后快速实施应急处置；
c) 支持对安全事件处置过程及结果进行记录，及时生成处置报告。

7.4.2 增强要求

无。

7.5 平台容灾备份

7.5.1 一般要求

应满足以下要求：

a) 建立备用通信服务，当主通信服务不可用时，确保平台用户在满足业务需求的时间段内通过备用通信服务访问平台；
b) 支持平台数据级容灾；
c) 支持对灾难备份和恢复过程进行记录；
d) 支持容灾恢复速度/时间符合合同或服务水平协议的约定。

7.5.2 增强要求

应满足以下要求：

a) 支持应用级容灾；
b) 支持异地容灾。

7.6 用户数据保护

7.6.1 一般要求

对平台用户网站数据应满足以下要求：

a) 明确用户网站数据归属于用户，不提供给任意第三方；

b) 支持用户数据隔离，平台用户仅能访问自身的安全防护资源；

c) 支持在法律法规允许范围内留存用户数据，并支持平台用户自定义保存期限；

d) 使用平台用户网站数据（包括数据衍生品），应事先取得用户授权，且数据仅可用于漏洞分析、攻击数据挖掘等提升平台安全防护能力的过程；

e) 支持用户退出平台服务时移交平台用户网站数据，并销毁其所有网站数据。

7.6.2 增强要求

无。

7.7 审计

7.7.1 一般要求

应满足 GB/T 31168—2014 中 11.1.1、11.2.1、11.3.1、11.7.1 和 11.11.1 的一般要求。

7.7.2 增强要求

应满足 GB/T 31168—2014 中 11.2.2、11.3.2、11.7.2 的增强要求。

参 考 文 献

[1] GB/T 28451—2012 信息安全技术 网络型入侵防御产品技术要求和测试评价方法

[2] GB/T 28827.1—2012 信息技术服务 运行维护 第1部分:通用要求

[3] GB/T 30276—2013 信息安全技术 信息安全漏洞管理规范

[4] GB/T 32914—2016 信息安全技术 信息安全服务提供方管理要求

[5] 中央网络安全和信息化领导小组办公室.国家网络安全事件应急预案.2017-01-10.

[6] NIST SP800-53-r4 Security and Privacy Controls for Federal Information Systems and Organizations, June 2013.