ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32924—2016

信息安全技术　网络安全预警指南

Information security technology—Guideline for cyber security warning

2016-08-29 发布　　2017-03-01 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

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　网络安全预警分级 …… 2
4.1　网络安全预警分级要素 …… 2
4.2　网络安全预警级别及判定 …… 3
5　网络安全预警流程 …… 4
5.1　预警的发布 …… 4
5.2　预警的响应与处置 …… 4
5.3　预警的升级或降级 …… 5
5.4　预警的解除 …… 5
参考文献 …… 6

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:国家网络与信息安全信息通报中心、公安部第三研究所、中国科学院软件研究所。

本标准主要起草人:黄小苏、张秀东、崔保红、陈长松、杜佳颖、连一峰、张海霞。

引　言

随着信息技术的广泛应用与快速发展，传统业务与信息系统的融合程度不断加深，网络安全对国家政治、经济、文化、公共服务活动的影响进一步增大。网络安全形势日趋复杂，安全威胁不断变化，利用网络漏洞、恶意程序从事入侵、破坏的活动频繁发生，不仅会造成信息泄露、数据篡改或丢失、服务拥塞、系统崩溃或硬件永久损害，甚至会对国家关键信息基础设施造成重大破坏，严重危害国家安全、公共安全和民众利益。

在网络安全防护工作中，社会公众在了解网络安全事件或威胁的基本情况，判断严重程度方面存在困难，对网络安全事件或威胁缺乏科学评估；另一方面，重要信息系统运营使用单位、网络安全企业和科研机构多仅从技术层面判断网络安全事件和威胁的影响。为进一步明确网络安全事件或威胁的重要程度和可能造成的影响，规范网络安全预警工作，有效开展处置工作，切实维护信息基础设施安全、公共安全和国家安全，推动我国网络安全监测预警机制的建立，制定本标准。

信息安全技术　网络安全预警指南

1　范围

本标准给出了网络安全预警的分级指南与处理流程。

本标准为及时准确了解网络安全事件或威胁的影响程度、可能造成的后果，及采取有效措施提供指导，也适用于网络与信息系统主管和运营部门参考开展网络安全事件或威胁的处置工作。

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 22240—2008　信息安全技术　信息系统安全等级保护定级指南

GB/T 25069—2010　信息安全技术　术语

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。为了便于使用，以下重复列出了GB/T 25069—2010 中的某些术语和定义。

3.1

网络安全保护对象　object of cyber security protection

亦指资产，对组织具有价值的信息或资源，是安全策略保护的对象。

注：主要指重要信息系统的应用、数据、设备。

[GB/T 20984—2007，定义 3.1]

3.2

网络安全威胁　cyber security threat

对网络安全保护对象可能导致负面结果的一个事件的潜在源。

注：例如，计算机恶意代码、网络攻击行为等。

3.3

攻击　attack

在信息系统中，对系统或信息进行破坏、泄露、更改或使其丧失功能的尝试(包括窃取数据)。

[GB/T 25069—2010，定义 2.2.1.58]

3.4

网络安全事件　cyber security incident

由于自然或者人为以及软硬件本身缺陷或故障的原因，对网络或信息系统造成危害，或对社会造成负面影响的事件。

3.5

预警　warning

针对即将发生或正在发生的网络安全事件或威胁，提前或及时发出的安全警示。