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

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。

4 网络安全预警分级

4.1 网络安全预警分级要素

4.1.1 概述

网络安全预警的分级主要考虑两个要素：网络安全保护对象的重要程度与网络安全保护对象可能受到损害的程度。

4.1.2 网络安全保护对象重要程度的判定

网络安全保护对象的重要程度根据其所承载的业务对国家安全、经济建设、社会生活的重要性以及业务对其依赖程度，划分为特别重要、重要和一般三个级别。

具体为：

a) 特别重要的保护对象，包括：
   ——按照 GB/T 22240—2008 的规定定级为四级及四级以上的信息系统；
   ——用户量亿级或日活跃用户千万级的互联网重要应用；
   ——日交易量亿元级的电子交易平台；
   ——行业占有率前五的互联网重要应用；
   ——提供互联网支撑服务的重要系统，如域名解析服务；
   ——由多个重要的网络安全保护对象共同组成的群体；
   ——其他与国家安全关系密切，或与经济建设、社会生活关系非常密切的系统。
b) 重要的保护对象，包括：
   ——按照 GB/T 22240—2008 的规定定级为三级的信息系统；
   ——用户量千万级或日活跃用户百万级的互联网重要应用；
   ——日交易量千万元级的电子交易平台；
   ——行业占有率较高的互联网应用；
   ——涉及大量个人信息的系统；
   ——由多个一般的网络安全保护对象共同组成的群体；
   ——与国家安全关系一般，或与经济建设、社会生活关系密切的系统。
c) 一般的保护对象，包括：
   ——按照 GB/T 22240—2008 的规定定级为二级及二级以下的信息系统；
   ——其他公共互联网服务等。

判定网络安全保护对象的重要程度宜综合考虑其所服务的用户量、日活跃用户数、交易额、信息安全等级保护的级别、数据敏感程度等因素。在重大活动期间，保护对象的重要程度宜适当进行调整。

4.1.3 网络安全保护对象可能受到损害程度的判定

网络安全保护对象可能受到损害的程度是指网络安全事件或威胁对其软硬件、功能及数据的损害，导致系统业务运行缓慢或中断，数据泄露、篡改、丢失或损坏，对保护对象造成直接及间接损失的程度。其大小主要考虑保护对象自身可能的直接损失，以及防御攻击、恢复系统正常运行和消除负面影响所需付出的代价，划分为特别严重、严重、较大和一般。

具体为：

a) 特别严重的损害，是指可能造成或已造成网络或信息系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除负面影

响所需付出的代价十分巨大。例如：

——大规模、持续性的网络攻击，可能造成或已造成网络或信息系统大面积瘫痪，使其丧失业务处理能力；

——涉及管理权限的安全漏洞及漏洞利用过程被披露，并出现自动化攻击工具，可能造成或已造成大规模个人信息泄露，包含账号密码、银行卡号等可能影响财物的信息。

b) 严重的损害，是指可能造成或已造成网络或信息系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除负面影响所需付出的代价巨大。例如：

——有组织的、针对性的攻击，可能造成或已造成网络或信息系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响；

——涉及远程命令执行的安全漏洞及漏洞利用过程被披露，可能造成或已造成大规模个人信息泄露，但不含财物信息。

c) 较大的损害，是指可能造成或已造成网络或信息系统中断，明显影响系统效率，使其业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除负面影响所需付出的代价较大。例如：

——针对性的攻击，可能造成或已造成保护对象网络和系统中断，明显影响系统效率，使其业务处理能力受到极大影响；

——涉及远程数据读取的安全漏洞被披露，可能造成或已造成个人信息泄露。

d) 一般的损害，是指可能造成或已造成网络或信息系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除负面影响所需付出的代价较小。例如，造成保护对象网络和系统短暂中断，影响系统效率，使其业务处理能力受到影响。

判定网络安全保护对象可能受到损害的程度宜从网络安全威胁本身和网络安全保护对象等方面考虑：

——网络安全威胁方面包括攻击者能力、攻击工具、攻击行为破坏性等；

——网络安全保护对象方面包括脆弱性严重程度、防护措施、攻击造成的损失程度等；

——其他，例如数据泄露的程度等。

4.2 网络安全预警级别及判定

4.2.1 概述

网络安全预警级别根据网络安全保护对象的重要程度和网络安全保护对象可能受到损害的程度分为四个级别：红色预警、橙色预警、黄色预警和蓝色预警。

4.2.2 红色预警（Ⅰ级预警）

当发生极其严重的网络安全事件或威胁，可能极大威胁国家安全、引起社会动荡、对经济建设有极其恶劣的负面影响，或严重损害公众利益，应发布红色预警。即可能对特别重要的网络安全保护对象产生特别严重的损害。

4.2.3 橙色预警（Ⅱ级预警）

当发生严重的网络安全事件或威胁，可能威胁国家安全、引起社会恐慌、对经济建设有重大的负面影响，或损害公众利益，应发布橙色预警。包括以下情况：

a) 可能对特别重要的网络安全保护对象产生严重的损害；

b） 可能对重要的网络安全保护对象产生特别严重的损害。

4.2.4 黄色预警（Ⅲ级预警）

当发生较严重的网络安全事件或威胁，可能影响国家安全、扰乱社会秩序、对经济建设有一定的负面影响，或影响公众利益，应发布黄色预警。包括以下情况：

a） 可能对特别重要的网络安全保护对象产生较大或一般的损害；

b） 可能对重要的网络安全保护对象产生严重或较大的损害；

c） 可能对一般的网络安全保护对象产生特别严重或严重的损害。

4.2.5 蓝色预警（Ⅳ级预警）

当发生一般的网络安全事件或威胁，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但可能对个别公民、法人或其他组织的利益会造成损害，应发布蓝色预警，特别轻微的可以不发预警。包括以下情况：

a） 可能对重要的网络安全保护对象产生一般的损害；

b） 可能对一般的网络安全保护对象产生较大或一般的损害。

4.2.6 网络安全预警分级表

由网络安全保护对象的重要程度与网络安全保护对象可能受到损害的程度确定的网络安全预警级别见表1。

表1 网络安全预警分级表

网络安全保护对象的重要程度	网络安全保护对象可能受到损害的程度			
	特别严重	严重	较大	一般
特别重要	红色预警（Ⅰ级）	橙色预警（Ⅱ级）	黄色预警（Ⅲ级）	黄色预警（Ⅲ级）
重要	橙色预警（Ⅱ级）	黄色预警（Ⅲ级）	黄色预警（Ⅲ级）	蓝色预警（Ⅳ级）
一般	黄色预警（Ⅲ级）	黄色预警（Ⅲ级）	蓝色预警（Ⅳ级）	蓝色预警（Ⅳ级）/无预警

5 网络安全预警流程

5.1 预警的发布

网络安全预警应由国家授权的预警发布机构发布。网络安全预警发布内容宜包含预警级别及其事件性质、威胁方式、影响范围、涉及对象、影响程度、防范对策等信息。

5.2 预警的响应与处置

网络与信息系统的主管和运营部门接到网络安全预警后，宜进行如下操作：

——分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度；

——将研判结果向上级及主管部门汇报；

——经上级及主管部门同意后，采取适当形式发送预警或通告给相关用户；

——根据情况启动应急预案。

当可能对网络与信息系统保护对象产生特别严重的损害时，网络与信息系统的主管和运营部门应

及时向单位负责人和信息安全第一责任人汇报。

5.3 预警的升级或降级

预警发布机构根据网络安全事件或威胁的动态变化，及时发布预警的升级或降级信息。

5.4 预警的解除

当网络安全威胁情况消除或威胁达不到蓝色预警级别，预警发布机构宜及时解除预警。

参 考 文 献

[1] GB/T 20984—2007 信息安全技术 信息安全风险评估规范