深度 |《网络产品安全漏洞管理规定》全面解读

Original 安恒信息 安恒信息 Today

背景介绍

2021年7月13日，工业和信息化部、国家互联网信息办公室和公安部三部联合发布了**《网络产品安全漏洞管理规定》**（以下简称《规定》），自2021年9月1日起施行。

此次规定中规范了漏洞发现、报告、修补和发布等行为，明确网络产品提供者、网络运营者以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人的责任与义务，将推动网络产品安全漏洞管理工作的制度化、规范化、法治化，提高相关主体漏洞管理水平，引导建设规范有序、充满活力的漏洞收集和发布渠道，防范网络安全重大风险，保障国家网络安全。

法规解读

《规定》指出，**国家互联网信息办公室**负责统筹协调网络产品安全漏洞管理工作。**工业和信息化部**负责网络产品安全漏洞综合管理，承担电信和互联网行业网络产品安全漏洞监督管理。**公安部**负责网络产品安全漏洞监督管理，依法打击利用网络产品安全漏洞实施的违法犯罪活动。

任何组织或者个人不得利用网络产品安全漏洞从事危害网络安全的活动，不得非法收集、出售、发布网络产品安全漏洞信息；明知他人利用网络产品安全漏洞从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

除以上提出规定外，对网络产品（含硬件、软件）提供者和网络运营者，以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人**三类目标群体**做出以下规定：

网络产品提供者

1、接收留存：应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于6个月。

2、漏洞修补：对所提供的网络安全产品存在的漏洞应立即采取措施并组织对安全漏洞进行验证，告知安全漏洞和修补方式，并且提供必要的技术支持；当其上游产品或者组件存在安全漏洞时，应立即通知相关产品提供者。

3、漏洞报送：应当在2日内向工业和信息化部网络安全威胁和漏洞信息共享平台报送相关漏洞信息。

4、推进建议：鼓励网络产品提供者建立所提供网络产品安全漏洞奖励机制，对发现并通报所提供网络产品安全漏洞的组织或者个人给予奖励。

网络运营者

1、接收留存：应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于6个月。

2、漏洞修补：网络运营者发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时对安全漏洞进行验证并完成修补。

网络产品安全漏洞发现、收集的组织或个人

1、鼓励通报：鼓励相关组织和个人向网络产品提供者通报其产品存在的安全漏洞。

2、发布限制：

▹不得在网络产品提供者提供网络产品安全漏洞修补措施之前发布漏洞信息。

▹不得发布网络运营者在用的网络、信息系统及其设备存在安全漏洞的细节情况。

▹不得刻意夸大网络产品安全漏洞的危害和风险，不得利用网络产品安全漏洞信息实施恶意炒作或者进行诈骗、敲诈勒索等违法犯罪活动。

▹不得发布或者提供专门用于利用网络产品安全漏洞从事危害网络安全活动的程序和工具。

▹在发布网络产品安全漏洞时，应当同步发布修补或者防范措施。

▹在国家举办重大活动期间，未经公安部同意，不得擅自发布网络产品安全漏洞信息。

▹不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供。

法律法规的其他相关规定。

3、备案登记：任何组织或者个人设立的网络产品安全漏洞收集平台，应当向工业和信息化部备案。工业和信息化部及时向公安部、国家互联网信息办公室通报相关漏洞收集平台，并对通过备案的漏洞收集平台予以公布。

4、加强管理：从事网络产品安全漏洞发现、收集的组织应当加强内部管理，采取措施防范网络产品安全漏洞信息泄露和违规发布。

相关处罚

1、网络产品提供者未按本规定采取网络产品安全漏洞补救或者报告措施的，由工业和信息化部、公安部依据各自职责依法处理；构成《中华人民共和国网络安全法》第六十条规定情形的，依照该规定予以处罚。

2、网络运营者未按本规定采取网络产品安全漏洞修补或者防范措施的，由有关主管部门依法处理；构成《中华人民共和国网络安全法》第五十九条规定情形的，依照该规定予以处罚。

3、违反本规定收集、发布网络产品安全漏洞信息的，由工业和信息化部、公安部依据各自职责依法处理；构成《中华人民共和国网络安全法》第六十二条规定情形的，依照该规定予以处罚。

4、利用网络产品安全漏洞从事危害网络安全活动，或者为他人利用网络产品安全漏洞从事危害网络安全的活动提供技术支持的，由公安机关依法处理；构成《中华人民共和国网络安全法》第六十三条规定情形的，依照该规定予以处罚；构成犯罪的，依法追究刑事责任。

漏洞管理的几点建议

《规定》依据《中华人民共和国网络安全法》制定,不仅是我们的指路灯,也是我们强有力的后盾。相关单位、平台和个人在收集、分析、留存、处理漏洞时，都应当依据《规定》建立健全的漏洞管理体系，采取相应措施确保漏洞信息的安全管理。

当前多数企业在实际环境中在作为网络运营者的同时也是网络产品的提供者，面临漏洞管理时需要解决以下问题：

- 漏洞与资产、人员、业务系统的关系梳理

- 基于人工的低效率漏洞梳理
- 针对存量的漏洞无法有效及时地形成跟踪数据
- 基于人工非标准化管理流程
- 法规要求的标准留存管理

形象的说，漏洞管理的首要目标是要**找到漏洞的归属人员，确立责任制**，在责任人进行整改的过程中，同步对漏洞进行整理分析，实时跟踪修复状态，同时对过程中产生的漏洞数据进行及时存留，建立完善高效的流程，做到**合法合规的漏洞管理**，因此可从以下几点入手：

建立清晰的资产管理档案

建立全生命周期的安全资产监控，监控资产的上线、变更、转移、报废信息，实时维护人员、业务系统、网络等多种重要因素，做到漏洞精准定位责任制。

高效的漏洞梳理

构建多来源漏洞统一管理和交叉漏洞验证体系，对多家厂商的扫描设备发现、多人员的渗透测试发现等方式的漏洞，集中标准化处理，提高漏洞发现的准确率，精简漏洞数量。

做精准的漏洞分析及跟踪

从披露漏洞开始，持续监控资产变化，实时获取漏洞披露情报，对漏洞发现、分析、修复和审核过程进行跟踪。通过对整个管理过程的评估、对比，达到持续优化漏洞管理的基准要求。

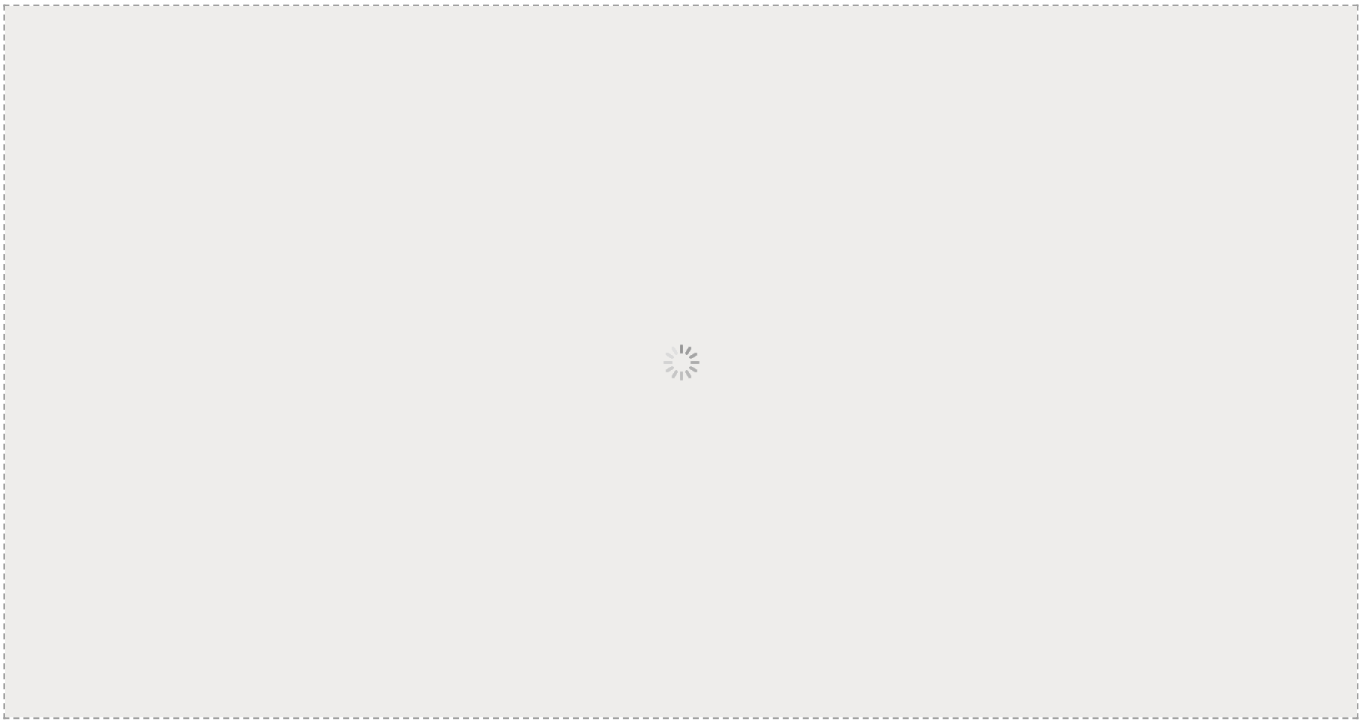
推动完善企业内部管理流程

基于企业内部管理流程，建立合适的漏洞流转流程，实现漏洞闭环管理、持续分析和预控安全风险，形成“管理层重视、一把手负责、全员参与”的管理模式。

标准化的漏洞留存

将以往漏洞进行标准化的留存，以满足法律法规要求，并在发现问题时能及时溯源追踪

当面临以上目标时，传统单一的扫描设备已不能满足漏洞管理的需求，在做好漏洞发现的基础上，需要通过**智能化管理平台**，在技术层面实现高效梳理、标准留存、完整闭环、自动化流转，以完成漏洞的**全生命周期管理**。



同时，结合企业目前现存的数据中台，如大数据平台、态势感知平台等高层分析平台，将漏洞、日志、流程、情报结合，进行**更高层次的数据安全价值实现**。

漏洞管理的未来

漏洞管理在未来仍是一个重大的挑战，随着5G、大数据、人工智能、物联网、云计算等相关技术的发展和应用，企业在数字化转型和应用的过程中面临着越来越多的安全风险和问题，安恒信息作为一家具有优秀企业文化和社会责任感的新时代网络信息安全产品和服务提供商，将“诚信正直，成就客户，责任至上，开放创新，以人为本，共同成长”作为企业的价值观,秉承“助力安全中国，助推数字经济”的企业使命，以“数字经济的安全基石”为企业定位，继续为网络安全做出贡献。

往期精选

围观 从防火墙、蜜罐到无所不在的迷网欺骗防御

热文 行业首批！安恒信息AiLand数据安全岛通过中国信通院权威评测

热文 亚运练兵 | 安恒信息护航"韵味杭州"田径邀请赛网络安全

People who liked this content also liked

一图+六问 | 读懂三部门《网络产品安全漏洞管理规定》

中国信息安全

《网络安全审查办法（修订草案征求意见稿）》为什么这样改？重点解读、前后对比

自主可控新鲜事

全文对比：《网络安全审查办法》修订草案都有哪些更新？

互联网安全内参