DOI：10.13955/j.yzyj.2022.03.12.05

信息安全风险指标体系研究与应用

冯哲夫

（中国邮政集团有限公司广东省信息技术中心，广东　广州　510898）

摘　要：从信息安全风险管理角度出发，构建信息资产风险的量化指标，从时间、危险程度、线性可叠加等角度进行脆弱性指标的设计，建立常态化的安全预警与监控体系，促进人员安全培训，提升安全整改的整体运作效率。

关键词：风险指标；安全监控；模型；脆弱性

中图分类号：F61　　**文献标识码：**A

1　信息安全风险指标构建的出发点

在信息安全风险管理中，通常要进行风险评估、风险减缓以及对风险处理进行决策，通过脆弱性量化风险评估，为后续的风险处理提供量化数据，促进风险减缓措施向高脆弱性、高威胁方向倾斜，从而降低整体风险，提升网络安全的保密性、完整性。

1.1　内部信息安全风险评价体系

信息安全风险指标可以直观地反映系统安全运行的情况，利用数据采集工具来收集被感知网络上的原始安全数据，通过数据处理，进行态势评估和计算，最终以数值或者图形的形式反映网络运行状况。指标反映出信息安全态势评估的决策思路和评估角度，影响着安全体系的应用范围和最终评估结果，对信息安全评估具有重要意义。

1.2　指标分类

根据现有安全体系研究基础和信息安全态势感知应用的实际情况，信息安全风险指标分为定性与定量两大类指标。

定性指标：对安全管理人员的知识量和经验有一定要求，主要采用模拟或者重现各种网络行为的方式进行评估。

定量指标：使用定量的指标体系数据，态势计算和评估结果最终以数值方式展示，如安全系数、网络节点权重、威胁度、网络性能监控数据等。定量安全态势指标划分为两类。一是基于安全风险的评价指标，它是体现信息安全的通用评估方法。通过将网络按照不同的层次结构进行划分，利用采集和检测工具收集各种网络攻击、日志信息和漏洞信息，通过一定的预处理和数学计算，将上述信息转化成信息安全态势量化数据，用于代表资产当前的安全状态，主要涉及主机脆弱性、攻击威胁度、漏洞利用等数据。二是基于网络和主机性能的评估指标，着重于对网络本省和网络节点性能进行态势评估，一般包括以下几种指标：网络端口流量、主机使用率、主机内存使用率、网络负载状况等。通过现有的网络监控系统或者检测系统等安全设备收集或者捕获网络和主机性能数据，并利用系统采集和分析功能得到日志统计信息。该类型指标需采集大量数据，整合应用复杂，审计规则简单，深层挖掘力度低，实时性不高。

获奖情况：2021 年全国邮政企业科技创新成果二等奖。

作者简介：冯哲夫（1978 ～），男，广东三水人，硕士，高级工程师，主要从事网络安全管理与研究。

收稿日期：2021－12－06　　**本刊网址：**yzyj.sjzpc.edu.cn

1.3　指标选定

邮政网络包括互联网、金融网、综合网、工控网、办公网等多种网络，选取主机、监控工具、网络设备为数据源，构建信息安全态势指标体系；实施自动采集，重点关注服务器脆弱性指标、终端脆弱性指标、代码漏洞数量指标、内部病毒感染率等。网络与主机性能指数则关注互联网异常访问数量、WAF检测异常数量、IDS异常数量等指标。在网络安全初级阶段，由于历史遗漏问题造成的漏洞较多，在同等威胁的情形下，应重点关注脆弱性指标，减少暴露的脆弱性，从而降低风险，提升网络安全能力。

2　脆弱性指标的设计

2.1　脆弱性指标的概念

脆弱性指标是评价某个服务器、某个区域、整体的脆弱性指标，代表受到内外部攻击的难易程度。

目前广东邮政应用PDCA流程对漏洞进行计划—漏洞检测—修复—复核实现闭环管理，在检测阶段使用绿盟Nsfocus、OpenVAS等漏洞发现工具对应用系统进行扫描，修复阶段委托开发团队、系统管理员进行修复，完成修复后再次进行复核，最后进行下一轮整改。

在PDCA循环过程中，由于系统数量多、人力资源少、漏洞种类多、修复时间长，需要聚焦以下三个方面：一是确定优先处理区域或者服务；二是评价系统脆弱性变化趋势；三是评价脆弱性修复效果。因此，需要构建一个量化指标作为标识，用于漏洞管理—修复流程，为安全管理人员提供导向性指引，促进漏洞修复，降低整体风险。

针对系统脆弱性采取一定防护措施，可以减少系统暴露在威胁下的可能性，从而降低系统风险。应对脆弱性的措施可以是安装软件补丁程序、修改配置、改变IT基础设施、更改流程等，也可以从管理、人员、技术防护等方面进行提升；通过漏洞扫描、系统监控等方式捕抓系统的脆弱性。

2.2　脆弱性指标的设计原则

通过设立脆弱性指标，从量化角度描述区域边界内系统的安全状况，为系统运维人员提供优先的漏洞修复指引。在管理角度则要求优先修复互联网边界、高风险、时间久远的漏洞。为了促进风险从高向低流动，形成指标驱动导向，在设计指标时需考虑以下原则。

量化性：风险以及脆弱性用数值表示。

促进性：对高安全等级、高风险、边界服务漏洞增加权重，形成风险梯度，促进优化方向从高向低转变。

时间性：尽量缩短脆弱性存在的时间。

最小资源：要求暴露面尽量少，尽量少提供互联网访问功能，尽量少开端口。

可叠加性：脆弱性模型可以采用线性叠加方式，支持风险区域的合并和拆分。线性叠加使得风险数值较为直观，让风险分析更加方便。

2.3　漏洞扫描工具

广东邮政采用的漏洞扫描工具主要有绿盟、OpenVAS、Nessus等，同时采用NMAP、Python等工具进行端口扫描及分析。

漏洞扫描软件（绿盟、OpenVAS等）采用CVSS评价体系（通用脆弱性评价体系）对系统进行评价。CVSS是一个开放的标准，可以对弱点进行评分，有助于判断修复不同弱点的优先等级。

CVSS从攻击途径、攻击复杂度、认证情况、机密性、完整性、可用性、漏洞所处生命周期进行综合评价。CVSS得分基于上述维度的测量结果，得分7～10的漏洞通常视为比较严重，得分在4～6.9之间的是中级漏洞，0～3.9的则是低级漏洞。

2.4　风险评估方法

2.4.1　风险评估概要

根据GB/T 20984—2007《信息安全风险评估规范》，系统风险与资产、风险、脆弱性三个因素有关，可以表示为：

风险值＝R（A，T，V）＝R（L（T，V），F（Ia，Va））

其中：R表示安全风险计算函数；A表示资产；T表示威胁；L表示威胁利用资产的脆弱性导致安全事件的可能性；Va表示脆弱性严重程度；Ia表示安全事件所作用的资产价值；F表示安全事件发生后造成的损失；V表示脆弱性。

《信息安全风险评估规范》并未指出具体的公式，下文将讨论L（T，V）指标的设计。参考

CVSS模型，该模型已经考虑到威胁利用脆弱性的评价，同时对脆弱性进行分析，可以使用L（T，V）表示静态的。由于威胁存在的时间越长，可能导致的风险越大，因此将威胁可能性增加一个时间因素P；同时高危漏洞应该比低危漏洞优先修正，而且高危漏洞权重应该优于时间因素权重。

2.4.2　脆弱性模型设计

以一个互联网系统为例，构建威胁—脆弱性模型：系统边界暴露在互联网的服务，内部脆弱性包括防火墙内开放的端口及服务。

假设时间威胁脆弱性呈线性增长，增长率为g/年，统计日期为D，那么该资源的威胁—脆弱性指标为：

$$L = p_1 L_{内} + p_2 L_{外} + p_3 \mathrm{E}$$

其中，$L_{内}$为内网脆弱性指标，$L_{外}$为外网脆弱性指标，E为端口数量，p_1、p_2、p_3为指标权重，可以针对应用状况自行设置，为了加强互联网的安全导向，应向互联网应用增加权重，可设置权重指标为：（p_1，p_2，p_3）=（1，2，1）。

考虑到CVSS线性增长设计（0～10的分值），实际上中等风险的漏洞比高风险漏洞数量会多1～2倍，为了促使高风险漏洞优先修复，引入风险权重指标c，每个漏洞权重如下：

$$c_i = \begin{cases} 3（7 \leqslant f_i \leqslant 10） \\ 1.5（4 \leqslant f_i < 7） \\ 1（0 \leqslant f_i < 4） \end{cases}$$

为了促进高安全级别系统的漏洞优先修复，引入安全级别权重指标h，针对互联网系统以及高安全级别的系统增加权重，h数值由系统安全定级决定：

$$h_i \begin{cases} 3（互联网系统） \\ 3（3级风险系统） \\ 2（2级风险系统） \\ 1（1级风险系统） \\ 1.5（未声明等级系统） \end{cases}$$

$L_{内}$为内网脆弱性指标：

$$L_{内}（T，V，P）= \sum_{i=1}^{n} (1+g)(D-y_{ni})\, f_{ni}\, c_{ni}\, h_{ni}$$

$L_{外}$为互联网脆弱性指标：

$$L_{外}（T，V，P）= \sum_{i=1}^{m} (1+g)(D-y_{mi})\, f_{mi}\, c_{mi}\, h_{mi}$$

其中，g为威胁—脆弱性随着时间的增长率（假定g=0.1），D为统计日期；y为漏洞的发现时间向量，y_i为漏洞i的发现时间；f_i为漏洞i的CVSS分数值，m为外网漏洞的数量；n为内网漏洞数量。

对于某个区域存在K个资源的情况下，各个资源的脆弱性之和就是该区域的脆弱性之和：

$$L_K = \sum_{j=1}^{K} L_j$$

2.4.3　总体风险指数

经过对省内各项基础设施的调研，目前广东邮政省中心已经构建了60多项风险指数，如机房制冷源风险、运维维保逆流程、网络负荷度、互联网系统受攻击数量、数据安全风险指数、系统运行风险、人员安全意识指数等，并构建总体风险指数，其公式如下：

$$L = \sqrt[n]{\prod_{n=1}^{n} \frac{100\,(L_i - L_{i\,max})}{L_{i\,max} - L_{i\,min}}}$$

其中，L_i为某项风险指数，$L_{i\,max}$、$L_{i\,min}$为该项风险指数期望的最高、最低风险值。采用各项风险指数的转换数值的几何平均值作为总体风险指数。

2.5　数据采集过程

2.5.1　内部资产发现机制

广东邮政设计了综合网、金融网全网段的扫描程序，工作时间捕捉省内所有网点、服务器的存活信息；捕捉每个机器的IP、操作系统版本、开放端口；通过模拟接入的方式，向每个开放的端口发送连接请求，获取每个端口的Banner（服务信息），获取该机器上部署的软件版本，同时将采集到的数据保存到数据库，以便未来开展硬件设备和软件资源在时间上的变化分析。

通过软件资产信息采集，初步采集了服务器类型（服务器、网络设备、终端）、软件服务端口、软件版本、操作系统版本数据，为漏洞更替、软件更新、操作系统升级提供了基础数据。

2.5.2　软件漏洞采集过程的自动化管理

为了实现漏洞发现—定位—修复—复核过程的自动化，减少人工操作的繁重任务，广东邮政在

省中心部署相应的绿盟漏洞扫描服务器，在绿盟服务器和各个网段之间使用一台可编程路由器控制绿盟服务器访问目标网络。省中心还部署了认证服务器、主控服务器、数据库服务器、FTP 服务器，支撑漏洞自动化扫描和分析，具体过程如下：一是扫描认证服务器接受各个系统管理员、安全管理员的漏洞扫描请求，并对每个请求进行登记，验证发送请求的用户身份，避免非授权用户进行漏洞扫描请求操作。二是主控服务器定期读取认证服务器上的漏洞扫描请求，在业务非繁忙时间修改路由器配置，允许绿盟服务器仅可访问有需要漏扫的服务器。三是绿盟服务器的定时任务执行漏洞扫描。四是通过在绿盟服务器配置自动上传服务，将扫描结果以 XML、Web Page 的形式传送到 FTP 服务器。五是主控服务器定时读取 FTP 服务器上的报告文件，执行文件的解压缩、读取文件。六是主控服务器将分析结果写入数据库服务器。七是报表服务器从数据库服务器读出漏洞数据，并进行报表展示。

3　预警体系组织架构与事件响应流程

3.1　常态化安全预警与监控工作

广东邮政省中心已经建立了常态化监控机制，每日发布安全预警。省中心每日进行持续的态势感知风险实时监控，执行 1 个频次的威胁情报（CVE 信息）采集工作、个频次的系统漏洞发布。同时，实行销号管理模式，对未销号的问题持续跟踪，每月根据整改情况，按照《信息网运行维护考核管理办法》实施考核。

安全预警的目标是在资产未受到安全攻击之前，对自身存在的客观漏洞进行预判，提前发现并修复；对正在发生的安全攻击及时发现和拦截。安全预警可缩短网络安全事件处理的时限，提升防守团队响应速度。安全预警过程整合了各类分析数据，安全预警处理过程贯通省市县网点，为邮政风险管控提供了实践标准，形成了一体化、标准化的处理流程。

威胁情报的获取来源于第三方服务以及开源信息。安全威胁预警依赖于情报采集，包括来自互联网、民间组织、政府机构、外部有偿服务提供的情报等。威胁情报来源有国家信息安全漏洞共享平台（CNVD）、通用漏洞披露（CVE）、Github 私人漏洞库、安全厂商付费漏洞库等。广东邮政采集的是 CNVD 漏洞库以及 Github 开源漏洞库。

3.2　事件响应流程

事件响应涉及全省的组织机构，形成多层级的处理组织。广东邮政建立了省中心—地市中心（直属单位）—区县—网点的整改链条。一个事件的发起从省中心开始，通过内部通信通知到地市中心，列出 IP、问题、现象等信息；地市中心启动 IP 定位查找工作，对涉事机器进行安全控制并开展修复工作。

事件处理响应时长是预警成败的关键。通过优化队伍配置，在省中心建立安全监控队伍，实现安全监控常态化从 0 到 1 的突破；建立全省安全监控的联络组织—问题定位—反馈机制，推动省直属单位、各地市分公司、省分行等单位协同作战；实行高标准整改期限制度：重大风险立即整改、高危风险 24 小时整改、中危风险 72 小时整改、低危风险 7 天整改。

事件处理与响应使用了发布、定位、修复、复核流程，依赖态势感知系统的安全管理模块，将每个事件进行流程化跟踪，当分派给地市中心处理时，省中心将事件状态修改为处理中，末端在规定的时间内完成修复后，省中心将进行事件复核，检测漏洞情况、观察异常流量，以判断该事件是否完成处理，确认完成后，省中心将事件状态修改为完成状态。预警体系事件流转过程见图 1。

3.3　全体员工安全培训

在安全管理中，最容易出现的是人员安全意识不足导致的风险。因此，广东邮政针对漏洞修复队伍、全体邮政从业人员进行安全培训。其中，安全意识培训覆盖到每一个人，通过建设中邮网院培训课程，强化风险意识以及防诈骗意识；针对省中心系统管理员以及地市管理员培训漏洞修复方法；使用现场培训、互联网培训等方式，多次组织超过百人的系统加固、终端修复等培训，提升员工的整体安全意识，提高管理员的安全技能。建立共享渠道，鼓励优秀单位分享整改经验，促进共同进步。

4　运行效果

信息安全风险指标体系包含了技术应用、安全管控流程、人员意识培训。通过构建信息安全风

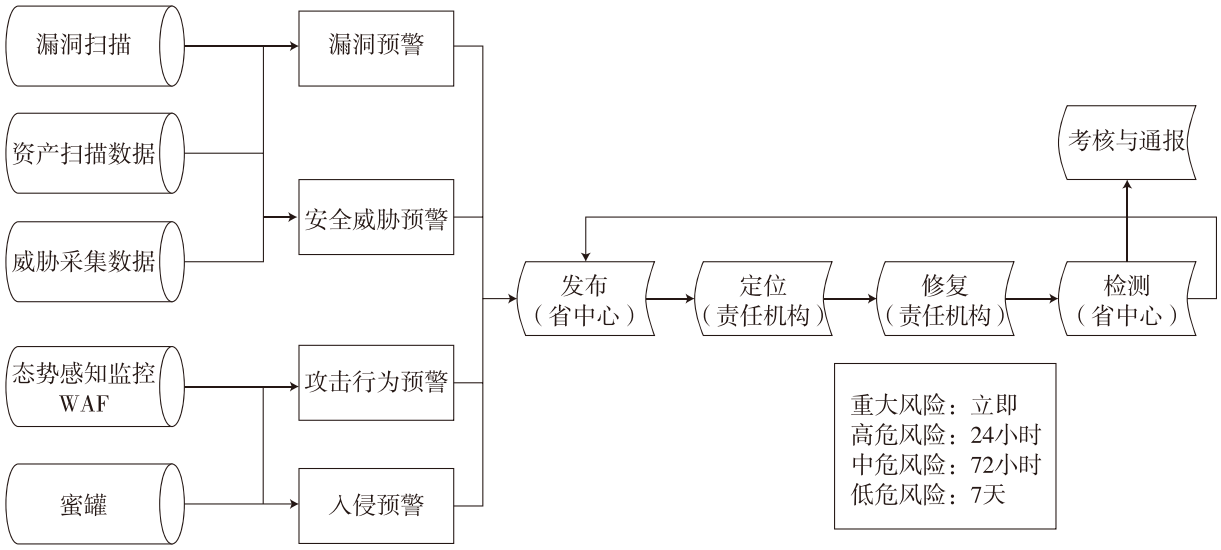

图 1　预警体系事件流转过程

险指标体系，广东邮政安全防护能力得到整体提升。

通过建立全自动化的内网、外网漏洞扫描，实现基于 NMAP、绿盟、交换机 MAC 采集等多来源的运维数据采集与整合。

建立全省统一资产库，为资产信息溯源提供了基础信息。累计发现 16 万个 IP，采集了 80 万个提供服务的端口信息。逐步建立了基于 IP 的信息资产表，为漏洞扫描提供了目标数据。

通过构建 CEV 基础信息库，采集了国家安全漏洞库数据，实现了资产与安全漏洞库的对比，改变了依靠漏洞扫描才能发现漏洞的情况，为互联网漏洞修复争取了时间。

构建了全省范围的安全响应机制，打造了安全整改的队伍，使得省内安全漏洞修复高效运作。制定了省内漏洞修复标准，实现省内安全监控常态化。

加强人员培训。2020 年广东邮政开展 2 次全员安全意识培训，开展 2 次终端漏洞修复培训，1 次 WAF 整改培训。

通过省分公司考核管理办法，每月对安全事件进行通报。将预警响应过程电子化、自动化、数据化。让积极投入的单位获得安全收益，让落后的单位得到提升，实现了经验共享。

从 2019 年至今，通过应用信息安全风险指标、建立全省安全运营体系、制定优化策略、确定优化区域、明确漏洞修复次序等措施，两年时间广东邮政省中心风险指数从 9 800 下降到 680，降幅 93.0%；地市中心风险指数从 6 542 下降到 358，降幅 94.5%；终端风险指数在 2021 年年内从 30 250 下降到 14 952，降幅 51%．全省中高危漏洞数量从 32 万个下降到 7 万个左右。

2021 年，广东邮政通过整合省内原有资产采集、自动漏洞扫描、外部资产发现等服务，省中心已经发现互联网、内网安全隐患 1 156 起，涉及病毒、弱密码、非法软件、互联网漏洞等，实现了网络安全防控和整治常态化，促进广东信息安全工作步入良态，及时处理率达到了 95% 以上，通过抓取 CVE 漏洞情报，可以在 3 天内与内网受影响的资产对比，缩短平均发现时长 30 天以上。

参 考 文 献

［1］国务院信息化工作办公室．信息安全技术 信息安全风险评估规范［S］．GB/T 20984—2007．2007—06—14

［2］王强，孟浩华．一种融合 CVSS 的信息安全终端安全评估模型［J］．计算机与数字工程，2016（4）

［3］计算机网络与安全．网络安全态势感知之态势指标构建［EB/OL］．https://www.sohu.com/a/331196064_653604，2019—08—02

［4］庄洪林，姚乐，汪生，等．网络空间战略预警体系的建设思考［J］．中国工程科学，2021（2）

［5］中国信息安全测评中心．中国信息安全测评中心［EB/OL］．http://www.cnnvd.org.cn/web/xxk/gyCnnvdJs.tag，2021—12—06