探讨信息系统安全等级保护测评的实施管理

卢荣森

广西信息安全测评中心　广西南宁

【摘要】信息系统安全是维护信息系统可持续性的重点工作，本文中笔者对当前我国信息系统等级保护测评工作中存在的问题进行了概述，并以此为基础提出了进行测评的标准过程及实施的范围和具体的测评方法。旨在为相关工作人员提供参考。

【关键词】信息安全；等级保护测评；信息系统

This paper discusses the implementation and management of information system security level protection evaluation

Rongsen Lu

Guangxi Information Security Evaluation Center, Nanning, Guangxi

【**Abstract**】Information system security is a key job to maintain the sustainability of information system. In this paper, the author summarizes the existing problems in the security work of information system level protection of our country, and puts forward the standard process, the range of implementation and the specific security methods based on it. The purpose is to provide reference for relevant staff.

【**Keywords**】Information security; Grade protection evaluation; The information system

引言

信息化社会中，小至人们的衣食住行大至国家的安全与发展，都离不开各类信息系统的支持。而信息系统的安全性则是确保信息系统可持续发展的重中之重。在我国信息安全领域，等级保护制度已经上升为一项基本国策。其关系到我国关键基础设施和信息资产的安全。在相关规范中，各类信息系统按照其重要性被划分为五个等级，并为每一个级别的信息系统提供了定级方案、安全建设、等级测评等。而其中最重要的则是等级测评，它几乎贯穿了整个信息系统的建设、应用、维护、退运等环节。当前，我国在长期的摸索过程中基本已经形成了一套等级保护标准体系。从实施反馈来看，这套体系较为完善各类测量实施工作的开展都基本做到了有据可依。但依旧存在部分问题有待解决，例如测评结果标准性不足，在一定程度上受到人为因素的影响以及数据管理效率低等。针对这些存在的问题，本文拟结合笔者参与的广西某电网公司信息安全等级测评实施经验，对当前该技术的应用问题进行分析，并提出一种可以量化的测评方法以降低人为因素的影响。

1 等级测评存在的问题

结合笔者自身的项目经验，认为在当前的等级测评过程中主要存在以下几个问题：

1.1 过度依赖测评师的个人能力

测评项目能否顺利实施以及测评结果是否准确，都几乎完全依赖于测评师的个人能力。笔者认为，这一现状的产生原因在于测评的标准化和全面性还不足，在很多时候迫使测评师不得不借助于个人经验临来进行测评。在测评遇到困难时，难以从相关的行业标准中找到解决的办法。过度依赖个人能力导致的问题是很严重的，首先是不利于检测结果的准确性，其次是检测效率低下不利于进行推广。

1.2 测评结果中，风险分析不够准确

在进行保护测评的过程中，对于发现的各类系统问题，测评师往往只对其进行了脆弱性划分，而对这个问题本身对系统产生的威胁分析不到位。产生这一问题的主要原因在于测评的方法非常单一，导致测评目标的表达既不及时也不全面。

1.3 测评效率较低

社会的信息化发展是在不断向前的，各类信息系统给传统行业赋能的步伐从未停止过。企业信息系统的总量迅速增加。尤其是对于有子公司和分公司的大型企业而已，其信息系统的测评难度极大，工作内容过度饱和。而当前的测评工作一部分还需要依赖于手工操作，且存在充分性。因此，亟需找到一种自动化的高效测评手段，来提升测评效率。

1.4 测评数据管理困难

准确获取各类测评数据是测评工作的主要目标之一，但是对于信息系统安全保护而言，获取测评数据只是工作的第一个环节。更重要的是对测评数据进行深入的分析，通过从不同维度的分析来为企业信息安全接触提供依据。但是目前，由于缺乏数据管理工具，因此数据分析的难度极大。

2 测评过程

基于以上问题，笔者拟定如下测评过程，以提升测评的规范化：

2.1 测评准备

在进行正式的测评之前，准备工作是必不可少的。准备工作的主要内容是对所需要的信息进行全面的搜集，并根据经验绘制出本次测评工作所需要的各类表单，以及在测试过程中所需要使用的各种测评工具等。需要注意的是，在准备阶段还要获取完整的资产信息表。而该表的形成需要在搜集所有资产信息的前提下对其属性进行赋值。对于信息系统而言，其资产往往被分为五个类别：系统、网络、介质、终端以及管理。良好的前期准备工作，是提升效率的有利途径。

2.2 编制测评方案

准备阶段搜集了大量的信息，这些信息将会被用于测评方案的编制。要对待测系统进行全方位的分析，找出与其相关的业务应用系统，并以此来确定测评对象。并对各项测评指标进行细化，选择最合适的测评工具，并拟定测试作业指导书，以便于实施人员参考。

2.3 现场测评

现场测评的开展依据是测评方案。在现场测评的过程中，要使用测评工具来取得相关信息，这些信息是后续进行数据分析的基础。现场测评的开展也可以进一步分为五个步骤：准备、实施、记录、确认、归还。在实施阶段，需要利用各种工具来对系统进行安全测试。测试的内容包括但不局限于漏洞扫描、渗透、病毒检测等。工具一般有 PC、抓包工具以及其他脚本等。在实施时，要根据具体的需求来选择最佳的方法和工具。在准备阶段进行选择，待实施完成后对过程与结果进行记录，确认记录无误后，归还各种硬件设备。

2.4 分析撰写测评报告

根据现场测评结果，通过一系列判定方法来找出被测评系统当前的安全保护现状，并将其与既定的保护要求进行对比，形成测评结论、完成测评报告。主要任务包括单项、单元测评结果判定、整体判定、风险分析等。

3 测评范围与方法

下面以某企业信息系统测评实例来进行测评范围与方法的论述：

3.1 测评指标

该信息系统安全保护分为两个主要部分，一是平台安全保护，二是业务信息安全保护。其中平台安全保护的等级为二级，服务安全保护的等级为三级。

3.2 测评对象

该系统的测评几乎覆盖了所涉及到的所有种类，其中重点测评的对象为硬件设备、基础设施、人员管理以及文档等。结合该系统具体的网络拓扑结构，本次测评工作的测评对象如下：

（1）主机房，主要测评内容包括机房内的整体环境、各类设施的保护情况等。

（2）存储被测系统重要数据的介质的存放环境。

（3）考察整个系统的网络拓扑结构是否完整，是否存在安全漏洞。

（4）各类安全设备的运行情况。

（5）对服务器的操作系统与数据库进行安全测评。

（6）管理终端测评。

（7）业务备份系统测评。

（8）对信息安全主管人员、各方面的负责人员等展开询问工作。

（9）对涉及到信息系统安全的所有管理制度和记录进行研究。

3.3 测评方法

（1）测评方式

①对相关责任人以及操作人员进行访谈。

②对系统环境、各类设备的运行状态进行核查

③测试及综合风险分析。

（2）测评工具

主要的测评工具采用铱迅漏洞扫描系统 NVS-2000。

（3）测评工具接入点的确定

结合系统的实际情况，本次测评过程的工具接入点选择在接入层的交换机。工具接入后，即开始进行模拟。模拟的主要内容是，外部或者内部恶意用户对操作系统、web 应用以及其他第三方产品进行恶意攻击。通过模拟找出可能存在的系统漏洞。并尝试能否利用这些漏洞来获取敏感信息、劫持数据以及获取控制权等。

4 单元测评

单元测评内容包括“基本指标”中涉及的安全层面。各个测评项在完成测评之后，会得出对应的分数。在单元测评中，将这些分数进行进一步处理，其方法是通过算术平均法来计算多个测评对象在同一测评项的得分。并将测评结果以表格的形式进行呈现，对于不同分数等级的得分，最好采用不同的颜色进行区分。通过表格可以直观的看出在单元测评结果中，哪些项是存在安全问题的。对于这些项，要进行进一步的抽取和汇总处理。汇总的结果是形成安全问题列表，并对表中的每一项进行计算，来评估其严重程度。计算公式如下：

安全问题严重程度值 =（5- 测评项符合程度得分）× 测评项权重。

从上述公式中可以看出，各项安全问题的严重程度是通过数字 1-5 来进行区分的，其中数值越大，则表示此项安全问题最为沿着。同时需要注意的是，在进行计算时，要结合测评项的权重来进行。

5 整体测评

整体测评从安全控制间、层面间、区域间和验证测试等方面对单元测评的结果进行验证、分析和整体评价。

5.1 安全控制间安全测评

该企业的机房位于公司主建筑的一楼，由于楼层较低因此存在受潮的风险。但在实际的检测过程中，发现该企业对机房做好了防风、防水、和防潮。从结果来看，能够有效规避此类风险，因此达到了等级保护的安全要求。

5.2 层面间安全测评

在检测的过程中，发现服务器的密码复杂的不够，且未使用密码复杂度策略。因此，要求企业提升服务器密码复杂度，并定期修改密码。

5.3 区域间安全测评

企业虽然开启了服务器的防火墙，但是防火墙版本较低，部分补丁未及时安装和更新。存在被扫描攻击以及木马攻击和服务劫持的风险。因此，提出建议更新补丁，并在网络边界上也部署防火墙。

5.4 整体测评结果汇总

评测得分有两个维度，一是初次测评的得分，二是修正后测评得分。根据这两个得分来形成最终的安全问题汇总表。具体实施如下：将各类控制措施的修正因子设置为 0.5-0.9。并以此计算：

修正后问题严重程度值 = 修正前的问题严重程度值 × 修正因子。

修正后测评项符合程度 =5- 修正后问题严重程度值 / 测评项权重。

6 安全状况分析

6.1 系统安全防护评估

将该系统采取的安全保护措施进行统计和汇总，形成统计表格。并将其按照控制点来进行打分，并转换为百分制得分。这样做的意义在于能够根据表格的内容，量化的对系统现有的保护措施以及存在的主要安全问题进行评价。

6.2 安全问题风险评估 ：

采用风险分析的方法进行危害分析和风险等级判定。以测评结果得分为基础，联系每一项存在的风险可能对系统造成的最严重危害来确定风险等级。该等级一般可以被划分为“高风险”、“中风险”以及“低风险”。

6.3 等级测评结论

综合上述测评与风险分析结果，根据符合性判别依据给出等级测评结论，并计算信息系统的综合得分。等级测评结论应表述为“符合、“基本符合”或者“不符合”。

结语

信息安全不是一个绝对的安全，也不存在绝对安全的信息系统。其安全是相对的，适度的整体安

全。因此，在对信息系统安全性进行评估时，不能武断的以“安全”和“不安全”来进行评价。同时，对于这种相对的安全性，也应该按照一定的标准来对其进行量化，通过具体的数据来描述系统的安全等级。同时应该认识到，安全等级保护测评是一项复杂的系统性工程，涉及到管理、技术以及法律等层面。随着信息系统的升级换代，该测评方法也应该出于动态的发展过程中，要进行不断的完善和持续性的改进。

参考文献

[1] 网络安全等级保护测评中的网络及通信安全测评[J]. 张珂.微型电脑应用. 2020(01)

[2] 总体国家安全观视域下我国网络意识形态安全问题研究[J]. 孙瑞婷. 广东行政学院学报. 2017(03)

[3] 网络安全等级保护 2.0 之常见安全要点及应对方法[J]. 李炜玥,冷昊,杨盛明,程德斌.电子质量. 2021(04)

收稿日期：2022 年 9 月 18 日

出刊日期：2022 年 10 月 25 日

引用本文：卢荣森，探讨信息系统安全等级保护测评的实施管理[J]. 国际计算机科学进展, 2022, 2(3) : 72-75.

DOI: 10.12208/j. aics.20220051

检索信息：RCCSE 权威核心学术期刊数据库、中国知网（CNKI Scholar）、万方数据 （WANFANG DATA）、Google Scholar 等数据库收录期刊