基于 CMDB 的资产识别与管理系统设计与实现

蔚周鹏[1],陈俊丽[1],张汉举[2]
(1. 上海大学 通信与信息工程学院,上海 200444;
2. 上海博弋信息科技有限公司,上海 200030)

摘　要:随着信息技术的迅速发展,针对企事业单位在资产识别与管理相关业务的开展过程中资产属性标准不健全、资产演变分析灵活性不足、安全分析不够完善等问题,设计基于配置管理数据库的资产识别与管理系统,推进企事业单位的资产信息化管理。该系统通过对资产信息的加工利用,覆盖到资产标准、资产质量、资产集成、资产安全等相关领域,充分标注资产各方面特征信息,完善了资产的演变分析。系统设计了一种安全分析计算的方法,收集资产的自有特征、脆弱特征、威胁特征完成资产的安全分析计算,通过信息安全技术方面的测试结果,明确目标资产自身的安全状态,及时对存在安全风险的资产采取合理的安全措施,对目标资产发生安全事件的可能性和抵御安全风险的能力做出评估。该系统应用突破了传统台账式资产管理,实现资产价值、脆弱和威胁的分析计算,对组织资产的信息安全建设有着积极推动作用。

关键词:资产识别与管理;配置管理数据库;演变分析;安全分析计算;信息安全
中图分类号:TP39　　**文献标识码**:A　　**文章编号**:1673-629X(2023)12-0106-07
doi:10.3969/j.issn.1673-629X.2023.12.015

Design and Implementation of Asset Identification and Management System Based on CMDB

WEI Zhou-peng[1], CHEN Jun-li[1], ZHANG Han-ju[2]
(1. School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China;
2. Shanghai Boyi Information Technology Co., Ltd., Shanghai 200030, China)

Abstract: With the rapid development of information technology, aiming at the problems of unsound asset attribute standards, insufficient flexibility of asset evolution analysis, and insufficient security analysis in the process of asset identification and management related business of enterprises and institutions, the asset identification and management system based on configuration management database (CMDB) is designed, which promotes the asset information management of enterprises and institutions. Through the processing and utilization of asset information, the system covers asset standards, asset quality, asset integration, asset security and other related fields, fully marks the characteristic information of all aspects of assets, and improves the evolution analysis of assets. The system designs a method of security analysis and calculation, which collects the asset's own characteristics, vulnerability characteristics, and threat characteristics to complete the security analysis and calculation of assets. Through the test results of information security technology, the security status of the target asset itself is clarified, and the existing assets with security risks take reasonable security measures to evaluate the possibility of security incidents and the ability to resist security risks of target assets. The application of this system breaks through the traditional ledger asset management, realizes the analysis and calculation of asset value, vulnerability and threat, and plays a positive role in promoting the information security construction of organizational assets.

Key words: asset identification and management; configuration management database; evolution analysis; security analysis and calculation; information security

0　引　言

大数据和云服务的快速发展促使企事业单位资产规模不断扩大,当前多数企事业单位的资产种类繁多、地点分散,资产信息的采集存在多个数据源,这些均加大了资产高效管理的难度。资产类别属性标准单一导致无法有效实施资产的量化管理。同时,多数组织未能对采集后的资产数据整合应用,不利于制定资产投入使用、日常维护及其变更等相关规划,未能有效挖掘

收稿日期:2023-02-06　　**修回日期**:2023-06-08
基金项目:国家自然科学基金(12174245)
作者简介:蔚周鹏(1997-),男,硕士生,研究方向为网络信息安全、信号处理;通信作者:陈俊丽,博士,副教授,研究方向为网络信息安全、智能信号与信息处理。

资产信息的价值。

CMDB[1-3] 全称是 Configuration Management Database,是一种配置管理数据库。英国国家计算机和电信局于 1999 年推出了 ITIL 的 V2 版本并提出了 CMDB 概念。CMDB 在实现资产精准管理和全面监控等方面发挥巨大价值,能够有效地组织各种形态的资产数据,释放资产信息价值。基于 CMDB 的资产识别与管理系统的设计实现企事业单位对资产的高效管理,通过识别、检查、维护资产资源,提供准确的配置信息给所需资产业务,从而落实全面、高效、可持续的面向业务服务的资产管理。多数企事业单位搭建的 CMDB 系统不能满足日常资产梳理的要求,也无法发现目标资产的威胁特征和脆弱特征,缺乏对资产信息的价值分析。市场上常用的 CMDB 软件有 OneCMDB,主要应用于中小规模公司,帮助组织管理多类软硬件资产,不过自动化导入只适配 Nagios 系统,局限性较大。

基于上述情况,该文设计了一种基于 CMDB 的资产识别与管理系统,建立了规范的资产属性标准,有效降低了资产维护的成本,提高组织内部的管理效能。资产识别[4]是实现企事业单位内部网络安全管理的关键步骤。本系统通过资产识别对目标信息系统的资产进行识别分析,形成对组织信息系统的基本认识。从资产管理[5-6]的角度来看,资产识别为企事业单位的资产管理工作提供信息基础。通过资产管理可以掌握组织内部的资产情况,当某资产存在漏洞,资产管理人员可以准确地做出响应措施,避免漏洞带来威胁。同时对闲置资产及时做出分析、处理,防止安全问题产生。并且,提出了一种资产安全分析计算的方法,对资产的价值、脆弱特征、威胁特征进行计算,帮助企事业单位组织开展风险评估[7-9]工作。

1　系统的设计实现

1.1　系统框架设计

资产识别与管理系统的建设通过规范化资产属性和功能模块的开发,实现资产信息同步变更,避免冗余资产数据堆积。系统整体框架如图 1 所示。

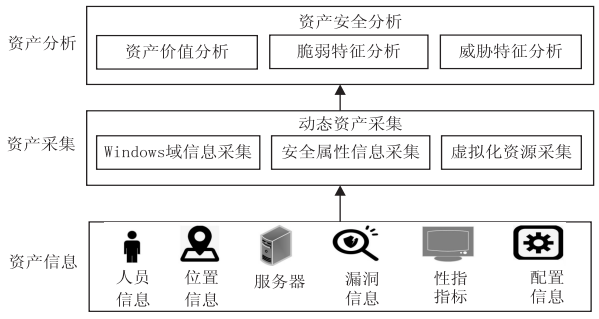


图 1　核心技术框架

由图 1 可知,本次系统设计首先基于各类资产信息,完成规范的资产属性设计,再从 Windows 域、安全属性信息、虚拟化资源中动态地获取资产信息,有效解决资产采集的瓶颈问题,实现资产快速准确的采集,最后针对资产当前的特征信息进行安全分析计算[10-14],有效解决了在资产管理过程中资产信息统计不精确、使用现状不清晰等问题。

1.2　资产安全属性的设计

通过对多家企事业单位资产情况调研,将收集的资产信息进行分析总结,建立了规范的资产属性,保持了资产数据的完整性。表 1 列出了本系统在目标资产属性与其它系统的对比。

表 1　资产属性对比

数据类型	属性信息	市场的 CMDB	本系统
基本数据	资产编号	√	√
	责任人	√	√
	资产名称	√	√
	资产状态	√	√
	资产环境	√	√
位置信息	所在城市	√	√
	所在街道/地点建筑物	√	√
	所在房间	√	√
	所在房间位置	√	√
参数数据	IP 地址	√	√
	开放端口	×	√
	端口数量	×	√
	端口服务	×	√
	网络区域	×	√
	所属业务系统	√	√
管理数据	部门	√	√
	资产类型	√	√
	人员管理	×	√
	资产分类与控制	×	√
	供应商	√	√
时间特性	上线日期	√	√
	变更次数	×	√
	重大变更日期	×	√
安全属性	漏洞总数	×	√
	告警总数	×	√
	保密性	×	√
	完整性	×	√
	可用性	×	√
	安全策略配置	×	√

由表 1 可知,市场的 CMDB 和本系统相比,在基本数据和位置信息两类属性信息基本一致,但参数数据、管理数据、时间特性和安全属性中的属性信息没有

本系统完善。故与其它平台属性相比,本系统设计的属性优点如下:

(1)提高了信息资产数据的使用效率;

(2)降低了后续数据的维护成本;

(3)考虑了资产的时间特性,捕获了资产的动态演变,帮助识别脆弱资产;

(4)加入安全属性,促进落实资产安全性评估。

1.3 动态资产收集

1.3.1 基于 Windows 域的信息采集

LDAP 是一种目录访问协议,在 Windows 域环境中基于该协议实现企业级的信息管理。基于 LDAP 协议框架的四种模型落实 Windows 基础域环境信息的查询与更新。LDAP 利用信息模型确认信息的表示方式和信息类型,使用规范的 Schema,加强信息之间的联通;利用命名模型确定协议中条目定位方式;在功能模型中实现域环境的信息操作,主要是查询类操作、更新类操作、认证类操作和其它操作;通过安全模型提供了基于 SSL/TLS 的通讯安全保障,加强了 Windows 基础域信息采集过程中的安全性,防止信息受到未经授权的访问。基于 LDAP 协议的 Windows 域信息管理,实现对公司所有用户账户、用户登录行为、密码状态、安全权限、组织单元架构、计算机、域控制器、工作站、组等信息的收集管理。图 2 为本系统对计算机对象累计登录次数的展示。

总计登录次数top10统计

name	登录次数	操作系统	系统版本,
NAS_	65535		
SS-XHDC	65535	Windows Server 2012 ...	6.3 (9600)
HYPERV-5	6973	Windows Server 2012 ...	6.3 (9600)
VCENTER	5876	Windows Server 2012 ...	6.3 (9600)
MYTH-WORKPC	2872	Windows 10 企业版	10.0 (19042)
WORKPC	1195	Windows 8.1 企业版	6.3 (9600)

图 2 计算机累计登录次数

图 2 记录了域中计算机对象的峰值登录次数,当组织内部出现关键登录事件时,对登录情况的记录分析能够帮助排查跟踪异常登录现象,判断是否存在违规行为。

1.3.2 安全属性信息采集

安全属性信息的采集对象主要是组织内部网络和服务的使用状况、脆弱特征、威胁特征等,对采集后的安全信息进行管理,为安全分析工作提供数据支撑。数据交互有 PUSH 模式和 PULL 模式,其中 PUSH 模式是监控对象主动推送数据,保证了信息的时效性,但是在数据量过大时,可能造成数据堆积,若处理不及时可能导致服务崩溃;PULL 模式是主动获取监控项指标,该模式下数据的利用性强,但是时效性一般。从数据完整性的角度来看,PULL 模式每次主动获取信息,明确信息完整度,若存在数据缺失也可及时做出分析处理;从灵活性的角度来看,PULL 模式在信息配置上明确自身指标,对信息完成二次加工利用。

结合实际环境,基于 PULL 模式实现安全属性信息采集,具体操作如图 3 所示,结合 CMDB 系统实现资产信息关联,完成信息加工。由图 3 可知,利用系统接口采集资产配置的弱点信息、漏洞信息[15]、网络异常行为以及资产性能信息等,落实资产脆弱特征和威胁特征的管理,并对其实现监控展示。

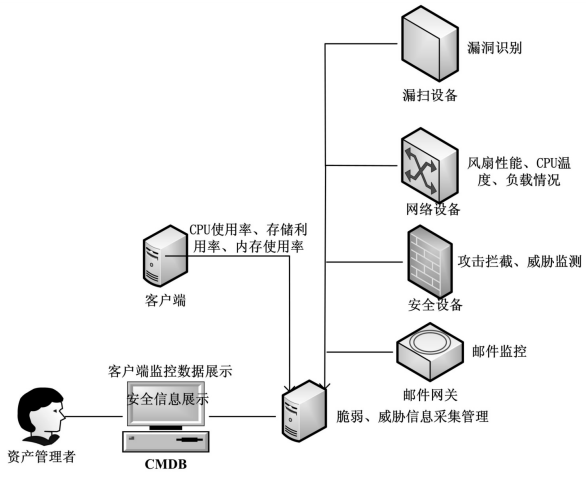


图 3 安全属性信息采集

在安全属性信息的采集管理下,针对漏洞信息的分析统计情况见表 2 中的漏洞信息统计。由表可知某制造业单位上海厂区的漏洞信息统计情况,汇总了上海厂区下各网段的存活主机数、高危漏洞覆盖主机数以及安全主机数。对高危漏洞进行排序后,通过漏洞信息的统计分析可以帮助该单位明确需要被优先解决的漏洞,最大限度地减少漏洞的威胁。

1.3.3 虚拟化资源采集

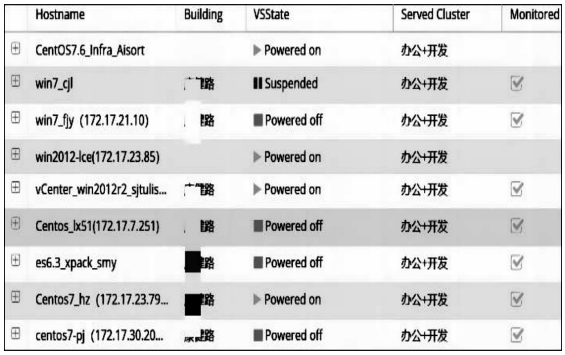
虚拟化资源采集的设计通过 REST API 接口实现了 CMDB 和虚拟资源信息之间的交互,REST API 是基于 HTTP 协议的 API,本次设计使用 HTTP 协议中的 POST、GET、PUT 以及 DELETE 等方法,实现用户对不同资源连接、管理等操作,其中数据的呈现方式为 JSON。REST 调用是无状态的,因此当出现故障,无状态组件可以根据实际环境开始状态转换来适应环境变化,故在资源管理中灵活性较高,同时具有简化的架构和改进的表示层,增强了后续二次开发的可扩展性。

基于 REST API 的开发,实现数据中心、集群、主机、虚拟机等信息的收集。在虚拟化资源应用下,对虚拟机相关属性信息的采集可如表 2 中虚拟资源信息统计所示。

由表 2 可知,通过对虚拟机状态及性能指标信息的采集,帮助落实可用性和性能方面的评估,降低了业务风险。方便管理员掌握虚拟环境的情况,避免闲置

资源堆积,让虚拟化环境保持高效运行。

表 2　采集信息统计

	漏洞信息统计	虚拟资源信息统计
信息采集		

1.4　资产安全分析

1.4.1　资产价值分析

ISO27001 规定数据资产具有保密性、完整性和可用性[16]3 个安全属性。保密性按目标资产若泄露对组织造成的损害程度进行评定;完整性按资产受到未经授权的修改对组织造成影响的严重程度来判定;可用性是按目标资产的可用度在正常工作时间所达比例或者允许中断次数来评估。上述 3 个属性对目标资产造成的影响程度决定了资产价值。资产价值计算如下:

$$a = \text{Round1}\left(\frac{T_C * \text{Conf} + T_I * \text{Int} + T_A * \text{Avail}}{T_C + T_I + T_A}\right) \tag{1}$$

其中,Conf 为保密性赋值;Int 是完整性赋值;Avail 为可用性赋值。Round1{ }表示四舍五入处理,保留一位小数;$0.5 \leqslant T_C, T_I, T_A \leqslant 1.5$,$(T_C + T_I + T_A) = 3$,$T_C$,$T_I$,$T_A$ 默认都为 1;资产价值的条件属性有保密性、完整性和可用性,管理者根据各属性的影响程度进行权重分配,完成资产价值的计算。本系统首先通过资产识别工作对资产进行分类梳理,然后在完成资产保密性赋值、完整性赋值和可用性赋值后便可开始资产价值的计算。同时,本系统结合实际情况对资产价值分析工作建立了统一标准,资产价值分析等级情况可如表 3 中资产价值部分所示。

1.4.2　脆弱特征分析

资产脆弱特征是资产在实际环境中存在的缺陷和弱点,主要从技术和管理两个方面考虑。技术层面脆弱特征从资产本身出发,如软件和系统上存在的漏洞;管理层面脆弱特征指结合资产的关联程度分析安全问题可能造成的危害。本系统对目标资产技术脆弱风险从漏洞角度考虑,按照漏洞危险程度和 CVSS 评分从高到低排列,漏洞风险值计算如下:

$$r_v = a_1 + \sum_{i=2}^{n}\left(\frac{a_i^{3.5}}{a_i^2} * \mu\right) \tag{2}$$

其中,$\frac{a_i^{3.5}}{a_i^2}$ 为影响系数,μ 为收敛系数。

被测对象的配置检查风险可以由具体检查结果和重要程度进行计算,计算方式如下:

$$r_b = \frac{\sum_{i=1}^{n} r_{bi}}{n} \tag{3}$$

$$r_{bi} = \frac{\sum_{i=1}^{l} w_i + \sum_{j=1}^{m} w_j}{\sum_{k=1}^{n} w_k} * 10 \tag{4}$$

其中,w_i 为不符合配置项的权重,l 为不符合配置项的个数;w_j 为部分符合配置项的权重,m 为部分符合配置项的个数;w_k 为配置项的权重,n 为所有配置项的个数。其脆弱值的计算如下:

$$v = w_v * r_v + w_b * r_b \tag{5}$$

针对不同配置检查项权重指标结合具体检查项进行调整,体现了重要程度不同的漏洞或者配置检查项对主机造成的影响。针对脆弱特征的分析,可知本系统首先在采集目标资产的脆弱特征信息后,完成资产的脆弱识别,再从目标资产的技术和管理两个层面上落实各自脆弱特征的计算,最后结合两者的计算值完成目标资产的脆弱特征计算。其中,脆弱特征的等级划分具体如表 3 中的脆弱特征部分所示。

1.4.3　威胁特征分析

威胁可能对资产造成损害,通常是安全事件发生的潜在原因。对威胁特征的分析[17],主要考虑它发生的可能性和造成的影响程度。威胁来源有多方面因素,包括人为因素和物理环境因素,归根结底,主要从内部(V_i)和外部(V_e)两个角度考虑。

$$T = V_i * W_i + V_e * W_e \tag{6}$$

结合实际情况,调整内部和外部威胁的对应权重完成威胁值计算。系统完成威胁特征信息收集后,开始对威胁特征进行识别,再从内部和外部两个角度取

计算目标资产的威胁特征值。同时,不同目标资产的内外部威胁权重也是不一样的,最后,对目标资产计算出的威胁值进行等级划分。对于资产价值、脆弱特征、威胁特征的等级划分情况如表 3 所示。

表 3 等级划分

	等级	价值/特征范围	标识	定义
资产价值	5	4.1-5	很高	重要程度很高,目标资产被破坏后可能导致非常严重的影响
	4	3.1-4	高	重要程度较高,目标资产被破坏后可能导致比较严重的影响
	3	2.1-3	中	重要程度一般,目标资产被破坏后可能导致中等程度的影响
	2	1.1-2	低	重要程度较低,目标资产被破坏后可能导致较低的影响
	1	0-1	很低	重要程度很低,目标资产被破坏后可能导致很低的影响
脆弱特征	5	8.1-10	很高	存在的脆弱特征级别很高,被威胁利用成功的可能性很高
	4	6.1-8	高	存在的脆弱特征级别较高,被威胁利用成功的可能性较高
	3	4.1-6	中	存在的脆弱特征级别中等,被威胁利用成功的可能性中等
	2	2.1-4	低	存在的脆弱特征级别较低,被威胁利用成功的可能性较低
	1	0-2	很低	存在的脆弱特征级别很低,被威胁利用成功的可能性很低
威胁特征	5	8.1-10	很高	威胁发生可能性很高,几乎不可避免
	4	6.1-8	高	威胁发生可能性较高,很有可能发生
	3	4.1-6	中	威胁发生可能性中等,可能发生
	2	2.1-4	低	威胁发生可能性较低,不太可能发生
	1	0-2	很低	威胁发生可能性很低,基本不会发生

由表 3 可知,资产价值的计算结果从高到低依次划分成 5 个级别,代表被评估资产的重要程度,主要依据目标资产被破坏后造成的影响来划分。其中,资产的重要程度越高,资产的价值就越高,被破坏后导致的影响也就越严重。脆弱特征的计算结果取值范围是 0 到 10,共划分成 5 个等级,分别代表着脆弱特征的不同级别,等级越高则代表该目标资产的脆弱特征级别越高,被威胁利用成功的可能性也就越高。威胁特征的计算结果可以划分成 5 个等级,不同等级代表威胁特征发生的可能性,级别越高则可能性越高,最高为 5 级,最低为 1 级。

2 结果分析与展示

2.1 资产动态演变展示

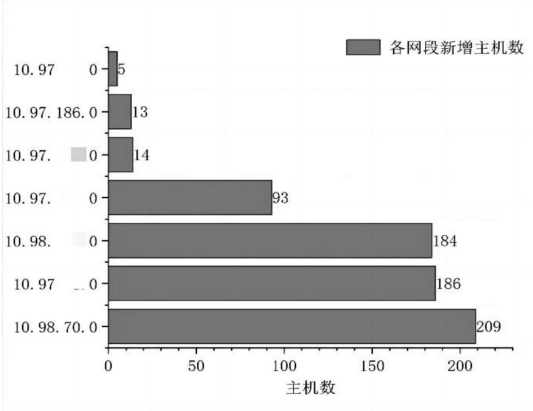
资产的动态演变可从网段、主机数等角度进行分析,本系统对某大型制造业企业上海厂区在 2021 年和 2022 年进行了年度资产检测,基于检测结果对资产演变做出分析展示。图 4 是 2022 年在网段、端口等方面的主机同比增量情况统计。由图 4 得出:

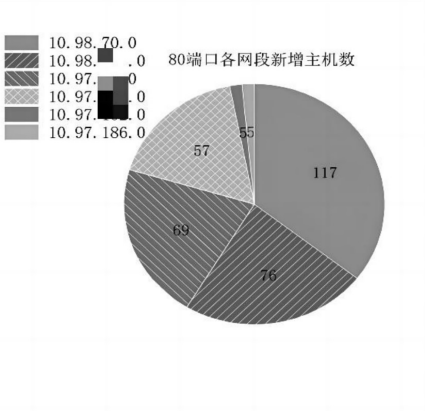
(1)相较于 2021 年,2022 年 10.98.70.0 网段新增主机数最多;

(2)2022 年内,开放 80 端口和 445 端口主机数相对 2021 年增加明显;

(3)该厂区 2022 年内业务快速扩张,其中网段 10.97.186.0 是非服务器网段,进一步分析发现该网段下存在主机开放的 80 端口并非业务所需,建议将该端口关闭,防止恶意攻击者对开放端口进行漏洞探测和漏洞利用。

综上,组织内部当前各网段主机数量的变化情况尚未超出内部的承载能力。基于演变分析明确了各网





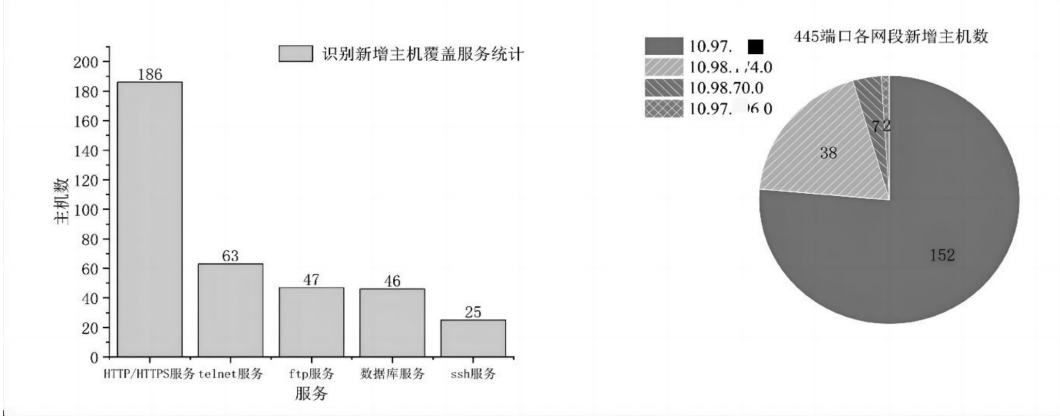


图 4　资产动态演变分析

段 IP 和端口的分布情况,帮助厂区核实排查,避免未授权端口出现使业务和数据受损,这是本系统开展资产动态演变分析工作的意义。

2.2　资产安全分析展示

现某企业实际资产评估[18-20]中,使用本系统开展资产安全分析工作。现选取部分资产进行分析,样例资产基本信息如表 4 所示。由表 4 可知样例资产的名称及其组成等基本信息,主要分为设备、软件和电子信息三类资产。表 4 中对资产选取的测试编号依次为 S1 到 S5,在后续的表格中将会以编号代表对应的资产。

表 4　样例资产安全分析结果

测试编号	资产类型	资产类别	资产名称	资产组成	C	I	A	存在的脆弱性	面临的威胁
S1	设备	终端设备(如笔记本/台式机)	个人办公电脑(台式电脑,笔记本电脑)	30 台台式电脑、27 台笔记本电脑	3	3	3	通过邮件可以将各类信息发送出去	信息泄露
S2	设备	安全设备	TDA	172.20.10.X	4	3	3	缺乏测试环境对新配置进行测试	配置错误影响正常工作
S3	设备	安全设备	机房设备(有监控)	监控摄像头、硬盘录像机、线缆等	2	3	3	存在高危漏洞	系统漏洞利用攻击
S4	软件	软件资产	系统软件	WIN7, WIN10, windows server 2008, win server2012	4	5	5	软件若保存至光盘/U 盘等实物,可能丢失;软件若保存在系统中,可能误删	软件丢失
S5	电子信息	数据	监控视频	监控视频数据	2	3	2	数据无备份	数据丢失

其中资产的保密性(C)、完整性(I)、可用性(A)以及存在的脆弱性和面临的威胁如表 4 所示。安全分析按照资产为中心的评估原则,利用本系统对其资产价值、脆弱特征和威胁特征进行计算,计算中考虑了各自特征主体或来源的不同,避免因资产特征的不同而造成误差,计算结果如表 5 所示。根据表 5 可知:

(1)编号为 S4 的系统软件资产重要性为 5,资产价值最高,其次是编号为 S2 的 TDA 设备重要性为 4,需要注意提高在企业中保护优先级;

(2)编号为 S3 的机房设备(有监控)的脆弱程度最高,级别为 4,其对应表 4 可知该设备存在高危漏洞,应及时修复,防止被恶意利用;

(3)其中,S1(个人办公电脑)、S3(机房设备)、S4(系统软件)、S5(监控视频)的威胁程度均为 3,要结合具体资产面临的威胁做好防护措施降低威胁发生的可能性。

表 5　资产安全分析计算结果

测试编号	资产价值	脆弱特征	威胁特征	资产重要性	脆弱程度	威胁程度
S1	3.0	3.1	5.5	3	2	3
S2	3.3	2.1	2.5	4	2	2
S3	2.7	7.1	5.5	3	4	3
S4	4.7	1.5	5.9	5	1	3
S5	2.3	4.5	5.1	3	3	3

结合表 4 和表 5 可知该企业设备、软件、电子信息三种类型资产的安全分析情况,如图 5 所示。

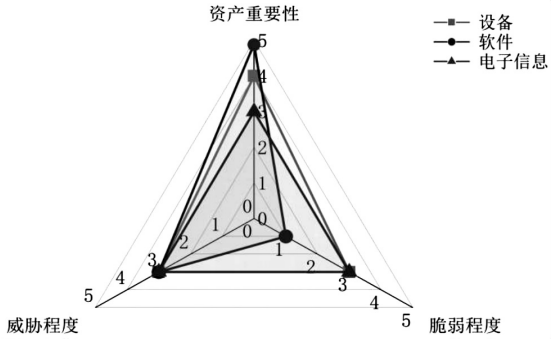


图 5 资产安全分析雷达图

由图 5 可知：

(1)当前设备类型资产重要性为 4，脆弱程度和威胁程度均为 3，建议对该类资产做安全加固；

(2)在该企业的所有资产中，软件类资产价值较高，重要性等级为 5，威胁程度为 3，注意降低软件保存介质为光盘、U 盘等实物存在丢失或者保存在系统被误删的可能性；

(3)电子信息类型的重要性、威胁程度、脆弱程度等级均为 3，需明确数据是否及时备份，防止数据丢失造成较大损失。

本系统通过资产价值评估促进资产优化配置，结合威胁程度、脆弱程度的评估结果明确目标资产发生安全事件的可能性和抵御安全风险的能力，对企业资产的安全状态做出判断。从信息安全体系建设角度来看，可以帮助组织做出预防性措施来降低安全脆弱性，做出保护性控制措施减少因威胁发生所造成的影响。

3 结束语

本次系统的设计，基于多家企事业单位的资产信息确定了各类资产对应的数据特征。系统支持动态采集各类资产信息，实现数据的实时更新，保证了信息的准确性和时效性，挖掘了资产信息的价值。系统中安全分析计算的设计为企事业单位针对资产的信息安全工作提供了数据支撑，当资产存在问题时，帮助技术人员及时明确资产责任人和所在位置等关键信息，避免造成更大的损失。本系统已在企事业单位中进行验证，帮助各组织有效推进资产信息数字化的进程。

参考文献：

[1] 王 磊，伍治平，成 名. 一种支撑云管理平台的 CMDB 设计方法[J]. 冶金自动化，2015，39(1)：13-18.

[2] 张亚辉，马海燕，陈 森，等. 设计运维一体化的 CMDB 数据库设计[J]. 长江信息通信，2021，34(12)：230-232.

[3] NA-LAMPANG N，VATANAWOOD W. Development of an ontology-based configuration management system[C]// 2016 8th international conference on electronics，computers and artificial intelligence (ECAI). Ploiesti：IEEE，2016：1-6.

[4] 赵庆聪. 基于业务战略的信息资产识别方法[J]. 北京信息科技大学学报：自然科学版，2014，29(1)：71-76.

[5] 邓 鑫，刘 然，贺俊彦，等. 基于 CMDB 的 IT 资产管理系统研究与应用[J]. 自动化应用，2020(8)：69-70.

[6] 高 凡，陈学卿，梁 强. 基于互联网的高校国资管理系统的设计[J]. 计算机技术与发展，2015，25(10)：174-178.

[7] ZHAO Xiangmo，DAI Ming，REN Shuai，et al. Risk assessment model of information security for transportation industry system based on risk matrix[J]. Applied Mathematic sand Information Sciences，2014，8(3)：1301-1306.

[8] 王雪莉，陈 刚. 云计算环境下信息安全风险评估流程探究[J]. 网络安全技术与应用，2020(11)：93-94.

[9] 邹 涛. 云计算环境下信息安全风险评估方法研究[D]. 南昌：南昌大学，2018.

[10] CHEN Xuexiu，CHEN Chi，TAO Yuan，et al. Cloud security assessment system based on classifying and grading[J]. IEEE Cloud Computing，2015，2(2)：58-67.

[11] 张楚渝，戴 菁，陈学海. 军事信息化的数据安全系统的研究[J]. 自动化与仪器仪表，2019(6)：212-214.

[12] FU C H，CHEN C Y. A study on decision-making opinion exploration in windows-based information security monitoring tool development[J]. Sustainability，2021，13(7)：3815.

[13] PAQUETTE S，JAEGER P T，WILSON S C. Identifying the security risks associated with governmental use of cloud computing[J]. Government Information Quarterly，2010，27(3)：245-253.

[14] 彭 勇，江常青，谢 丰，等. 工业控制系统信息安全研究进展[J]. 清华大学学报：自然科学版，2012，52(10)：1396-1408.

[15] 杨一未. 多因素漏洞评价方法研究[J]. 计算机技术与发展，2022，32(12)：88-94.

[16] 刘意先，慕德俊. 基于 CIA 属性的网络安全评估方法研究[J]. 计算机技术与发展，2018，28(4)：141-143.

[17] DAHBUR K，MOHAMMAD B，TARAKJI A B. A survey of risks，threats and vulnerabilities in cloud computing[C]// Proceedings of the 2011 international conference on intelligent semantic web-services and applications. [s. l.]：ACM，2011.

[18] 张 益，霍珊珊，刘美静. 信息安全风险评估实施模型研究[J]. 信息安全研究，2018，4(10)：934-939.

[19] 张 洋. 网络信息系统资产评估研究[D]. 北京：北京邮电大学，2013.

[20] GB/T 20984-2022，信息安全技术 信息安全风险评估方法[S]. 北京：国家市场监督管理总局，国家标准化管理委员会，2022.