

连锁经营企业网络安全评估模型研究

蔡京玫

(上海商学院 信息与计算机学院, 上海 2002352)

摘 要: 针对连锁经营企业网络独特性和当前主要网络安全评估模型局限性, 提出一种基于安全相似域的网络风险评估模型. 根据连锁经营企业内部网络拓扑结构特点, 将评估网络环境中的要素按照安全风险值划分为安全相似域, 通过安全相似域的关联性计算, 量化评估网络的安全风险值. 通过对网络安全评估模型验证结果表明, 本文评估模型不仅具有较高的风险评估精度, 而且减少计算量, 具有一定的实用性.

关键词: 连锁经营; 网络拓扑; 网络安全; 评估模型

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)03-0014-04

Research on Network Security Evaluation Model of Chain Enterprises

CAI Jing-mei

(College of Information and Computer, Shanghai Business School, Shanghai 200235, China)

Abstract: Because the chain enterprise network is unique and the current main network security assessment model limitations, the paper proposed a chain business enterprise network security assessment model based on the networks similar domains. According to the chain enterprise internal network topological structure characteristics, the environment of the network is divided into similar security domain according to the security risk values, similar domain association is calculated, and network security risk values are quantitative evaluation. The network security assessment model is tested by experiments, the results show that, the proposed model not only has improved the risk assessment precision, but also reduces the amount of computation, it has a certain practicality.

Key words: chain business; network topology; network safety; evaluation model

1 引言

连锁经营是我国商业流通领域中一种主要业态和最具活力的经营方式, 企业内部的局域网和 Internet 是企业运作的核心基础设施, 网络上的资金流、商品流、物流和信息流的安全与畅通是企业正常运营的命脉. 然而每一个网络系统都存在脆弱性, 脆弱性被具有不良行为的攻击者所利用, 现代连锁企业信息系统庞大, 自动化程度高, 一旦遭到网络入侵, 会导致系统瘫痪, 给企业带来巨大经济损失^[1]. 连锁经营企业网络安全问题越来越受到人们的关注和重视, 如何对连锁经营企业网络安全进行准确评估, 成为能否保证企业正常运营的关键^[2].

针对企业网络安全评估问题, 国内外大量学者

对其进行广泛而深入研究, 提出了一些网络安全评估方法, 并取得了一些成果. 主要有前网络安全评估方法主要定性评估方法、定量评估方法和人工智能评估方法 3 大类^[3]. 然而专门连锁经营企业网络评估研究国内几乎没有. 从连锁经营企业各互联的局域网安全特征的独立性及网络主体安全的相关性出发, 本文提出基于安全相似域的网络风险评估模型, 并采用实例进行分析, 评价其有效性.

2 连锁经营企业网络安全问题描述

2.1 连锁经营企业网络拓扑结构

连锁企业由一个总部、多个区域配送中心或分销中心、多家门店组成, 地域上通常是非常分散. 根据连锁企业的组织结构和经营管理特征, 连锁经营

企业网络主要由总部(及信息中心)、分销或配送中心、门店三部分网络互联而成,如图1所示。

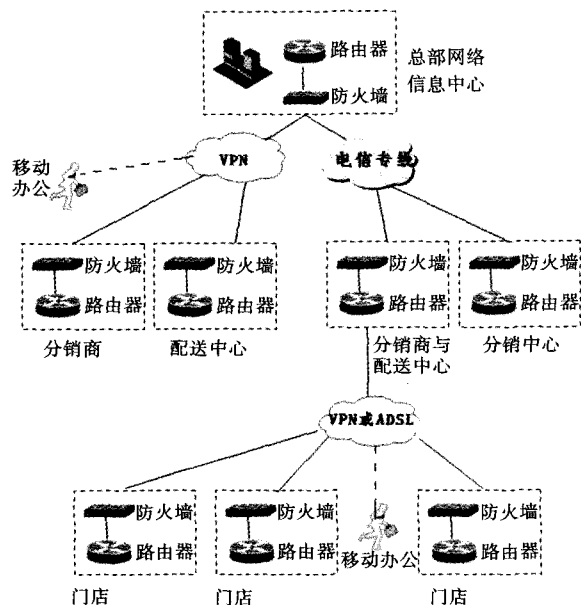


图1 连锁经营企业网络连接拓扑图

总部与区域分销(配送中心)通过专用通信网络互连,实现高速、安全的数据传输;分销商与配送中心和门店通过公用网互连,实现信息资源的交换;用户通过公用网连接到企业Web服务器;企业通过VPN或专线与外部供应商、银行或物流部门互连。

2.2 连锁经营企业网络威胁

为了保护现代连锁企业信息系统安全,企业网络一般进行加密、防火墙、口令认证、访问控制、防病毒软件等传统安全防护设施,以及入侵检测系统等安全防护机制,很大程度上保障了连锁经营企业网络信息的安全和畅通。但是由于各种原因,连锁企业安全问题仍然层出不穷。主要是由于部分员工缺乏信息安全意识;缺乏企业信息安全风险的识别、监测和控制管理体系;缺乏漏洞应对技术;缺乏信息安全内部统一的控制机制;无线网络、便携机移动办公和移动储存设备接入公司核心业务系统存在核心信息泄密风险;数据分级在公司内部没有严格控制;邮件、即时通讯、网页上传等文件外发存在信息泄密。要有效减少连锁经营企业网络威胁,必须对网络安全进行有效评估,发现已有和潜在网络安全问题,及采取控制措施,保证现代连锁企业信息系统正常运行^[4]。

3 连锁经营企业网络安全评估

3.1 网络安全评估模型

网络安全评估是一个综合评价过程,依据有

关网络安全技术标准和一定评估技术,对网络系统信息的完整性、保密性和可用性等进行科学评估,评估系统的脆弱性、面临的威胁以及脆弱性被威胁资源利用后所产生的实际负面影响,并根据安全事件发生的可能性和负面影响的程度来识别网络安全系统的安全风险。根据评估结果,提出有效的安全措施,消除风险或将风险降低到最低程度^[5]。连锁企业各互连的局域网存在异构性,信息资产的重要性等级不同,安全技术、安全管理以及安全策略实施不尽相同,评估准则和指标难以统一量化和操作,同时连锁企业网络安全具有不确定性、非线性及时变等特点,采用传统数学模型进行评估得到的结果正确率低。本文从连锁经营企业各互连的局域网安全独立性和网络主体安全的相关性特点,根据网络安全相似域理论对现代连锁企业网络安全风险进行评估,其评估模型如图2所示。

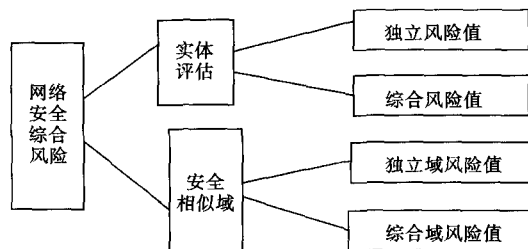


图2 网络安全评估模型

3.2 网络安全评估相关定义

基于网络安全相似域的现代连锁经营企业评估模型包括安全相似域构成,安全相似域由评估实体构成。

网络安全相似域定义为具有相似安全属性的实体组成的集合,其网络安全相似性由域隶属度来衡量,采用 U_j 来表示第 j 个安全相似域,那么如果 U_j 的隶属度大于某个预先设置的阈值就可以认为该实体是域 U_j 的成员。网络安全相似域的划分可从管理角度出发,如按照部门组织结构进行相似域来划分,即有:

$$U_j = \{u_{ij} \mid i = 1, 2, \dots, N\} \quad (1)$$

其中, u_{ij} 表示一个实体。

网络实体的独立风险值可定义为不考虑评估实体之间的相互影响的条件下,对某个网络评估实体进行风险评定所得出的结果,记为 RS 。

网络实体的综合风险值定义为考虑所有对某一评估实体安全产生影响的关联实体的风险影响,根据关联影响程度综合评定所得出,记为 RI 。例如企业内部运行各类数据库系统的服务器实体,其综合

风险必受到众多运行各种信息管理系统的服务器的分险影响,因此要综合考虑相关的影响。

网络安全相似域独立风险值是在考虑域内各评估实体安全关联的情况下,计算出来的网络安全风险值.网络安全相似域的综合风险是在考虑各相似域之间安全关联的情况下,计算出来的网络安全风险值.网络安全综合风险值在网络安全相似域的综合风险基础上,考虑网络外部的安全威胁。

安全相似域隶属度定义为某网络评估实体隶属于某安全相似域的程度,采用 I_{ij} 表示,即网络实体 i 隶属于安全域 j 的程度。

评估实体定义:现代连锁经营企业网络环境中的基本组成实体可以是主机、服务器、路由器、防火墙等,每一个实体又由软件、硬件、数据和服务等一部分或多部分组成,软件、硬件、数据和服务则由具体的资产组成.例如具体的软件资产可以是操作系统(如 Linux)、应用程序软件(如 MIS、DSS、Mysql),还可以是存放在实体上的源程序和数据(如商品库存)等;服务包括 ERP、POS 和 OA 等.因此可以用一维向量来描述系统中的每一个实体属性,即有:

$$\{ID, U_j, RS, RI, e\} \quad (2)$$

其中, ID 表示是网络评估实体标识; U_j 表示网络安全相似域标识; RS 表示该实体的独立风险值; RI 表示该实体的综合风险值;属性 e 为该实体对其所属的相似域的隶属度。

3.3 网络安全相似域的划分

借鉴 ISO17799 的资产确定思想来确定实体独立风险值计算时需要考虑的因素,并为底层资产赋值.底层资产的风险值由底层资产的属性风险值和底层资产的属性权重决定^[6].属性风险值是指资产的(机密性/完整性/可用性)遭受威胁时对系统造成的影响的量化衡量.各个属性风险值视该属性遭受威胁时对系统造成的危害分 5 级进行赋值,分别是: {可忽略、低、中等、高、极高}。如图 3 所示。

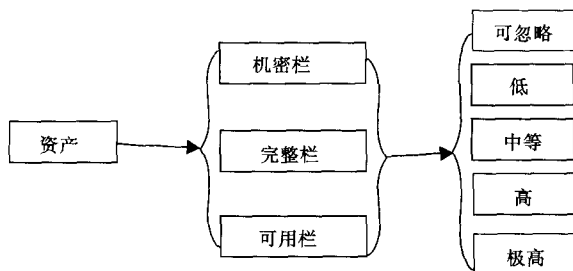


图3 网络安全风险资产风险赋值准则

网络安全风险资产属性风险值可采用一维向量描述为:

$$RS_{attr} = [R_{secret}, D_{integert}, D_{avaiable}] \quad (3)$$

风险属性权重是各个安全属性在资产风险值衡量中所占的比重.例如,对于 Mysql 数据库来说,如果其中存储的是敏感数据,则数据的机密性所占的权重较大;而如果存储的是校验数据,则数据完整性的权重就需要优先保证;资产的属性权重也可以表示为一维向量^[7]。

$$RS_{wattr} = [W_{secret}, W_{integert}, W_{avaiable}] \quad (4)$$

网络安全资产风险值计算公式如下:

$$RS = RS_{attr} * RS_{wattr} \quad (5)$$

最后,使用加权平均法计算实体的独立风险值(RS),加权平均法的公式如下:

$$RS = \sum_{i=1}^n RS_i * w[i] \quad (6)$$

这样,通过式(6)可知,网络实体风险值为该对象所有子要素($i=1, 2, \dots, n$)风险值的加权平均,其中 $w[i]$ 表示上层实体的第 i 个子元素所占的权重。

将系统工作环境中的安全相似域划分为 5 个等级,每个等级包含一个或多个具有不同阈值的安全相似域.将环境中所有实体的独立风险值按照递增排序组成的增量区间 $[\min(RS), \max(RS)]$,近似地将值的变化模拟为一个连续的过程,然后取风险值增量,即有:

$$\Delta = \frac{[\min(RS) - \max(RS)]}{n} \quad (7)$$

划定相似安全域的阈值区间为:

$$[\min(RS), \min(RS) + \Delta, \dots, \max(RS)] \quad (8)$$

网络安全相似度定义为指网络评估实体间安全属性的接近程度,采用 L_{ij} 描述实体 i 与实体 j 之间的网络安全相似程度.设网络评估实体的安全属性集为 $\{x_1, x_2, x_3\}$,那安全相似度就可以视为这些网络安全属性的函数,则有:

$$L_{ij} = f(x_1, x_2, x_3) \quad (9)$$

那么通过式(10)计算出每一个网络实体的隶属度值。

$$\begin{cases} L_{ij} = 1 & \text{if } i = j \\ L_{ij} \in [0, 1] & \text{otherwise} \end{cases} \quad (10)$$

首先将需要评估的目标网络划分为有限个安全相似域,采用由有限个网络实体隶属度大于预先设定阈值组成网络安全评估实体组成的集合.网络安全风险评估网络的抽象示意图如图 4 所示.在图 4 中,每个安全相似域之间的有向直线表示域之间的

安全关联,每一个相似域内有许多个不同数目的评估实体^[8].

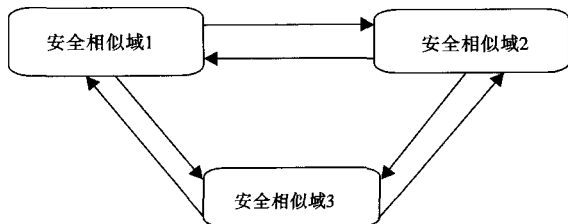


图4 相似安全域的划分和安全关联

根据域内实体之间的安全相似度计算出实体的综合风险值 RI 。

单向安全关联系数表示安全相似域 i 对安全相似域 j 的安全影响程度,采用 R_{ij} ,且当 $R_{ij} \neq R_{ji}$,且 $i = j$ 时, $R_{ij} = 1$ 。

在网络安全评估过程,采用关联系数矩阵来描述各安全相似域间的安全相互关联程度,采用 $R_{ij} = 1$ 。设网络中含有 n 个域,那么域安全关联系数矩阵表示为:

$$\begin{pmatrix} 1 & R_{12} & \cdots & R_{1n} \\ R_{21} & 1 & \cdots & R_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ R_{n1} & R_{n2} & \cdots & 1 \end{pmatrix} \quad (11)$$

3.4 网络安全风险评估过程

设待评估目标网络系统中共有 n 个安全相似域,通过计算域中的实体独立风险值加权评估值,则可以得到域独立风险值向量 $(RS_{u1}, RS_{u2}, \dots, RS_{um})$,采用全部安全相似域独立风险的算术平均值作为网络的风险值,记为 NRS 。

$$NRS = \sum_{i=1}^n RS_{ui} / n \quad (12)$$

设 R 表示相似域安全关联系数矩阵,那么自身风险和其它域对该域直接关联造成的风险的综合就是域 i 的综合风险值,具体计算公式如下:

$$RI_{ui} = \sum_{j=1}^n RS_j * R_{ji} \quad (13)$$

这样通过上述计算就可以得到该网络的域综合风险向量,即为域独立风险向量同域安全关联系数矩阵的乘积:

$$(RS_{u1}, RS_{u2}, \dots, RS_{um}) \times R_{mm} \quad (14)$$

网络综合风险值 NRI 为各域综合风险值的算术平均值,故求解如下:

$$NRI = \sum_{i=1}^n RI_i / n \quad (15)$$

4 模型的应用实例

4.1 网络安全相似域的划分

在调查了十一家不同规模(门店数为 10~100)的连锁经营企业网络后,所有的网络基本结构均为图 1 所示的结构子集。采用本网络安全评估模型对其中的 3 家(门店数为 50、30、10)连锁经营企业网络安全进行实证分析。为了减少计算量以及连锁经营网络各组成机构功能的明确分工,首先根据行政结构将总部、信息中心、分销商、物流配送中心、门店等局域网络设为安全相似域,如表 1 所示。

表1 安全相似域的划分

相似域标识	机构名称	备注
U1	总部	经营管理的核心
U2	信息中心	数据存储中心
U3	分销商	区域的管理中心
U4	配送中心	物流中心
U5	门店	销售中心
U6	第三方	供货、支付或运输
U7	移动办公	内部人员办公
U8	网络通信	第三方技术支持
U9	电子商务用户	普通消费者

根据经验确定每个安全相似域的安全目标,然后根据目标设定对应的安全等级(1~5 级),各机构内的评估实体相对于本机构的安全相似域的隶属度为 1。对于大型公司,在本级安全相似域下可以再划分 2 级安全相似域,2 级安全相似域划分时可以采用 3.3 节所述的模型划分 2 级安全相似域,可以提高评估精度。

4.2 网络安全模型的应用

分析各安全相似域中各实体的组成资产,如数据库系统、信息管理系统、经营数据、库存数据等,计算各实体的独立风险值,然后计算出实体的综合风险值,安全相似域的独立风险值和综合风险值,计算出网络安全的综合风险值。采用本模型的评估精度如表 2 所示。

表2 模型的评估精度

企业规模	安全相似域	风险等级
门店(50 家)	20	低
门店(20 家)	13	忽略
门店(10 家)	5	高

(下转第 21 页)

6 结束语

理论推导与仿真研究表明,利用小波分析和与鲁棒最小二乘法相结合的多传感器信息融合估计算法对参数进行检测,能够充分利用量测数据,将噪声最大程度的抑制.在估计的无偏性和均方误差最小的前提下,该方法表现出较好的稳健性和鲁棒性,是一种有效的土壤信息融合估计方法.

参考文献:

- [1] 庞凤,李廷轩,王永东,等.土壤速效氮、磷、钾含量空间变异特征及其影响因子[J].植物营养与肥料学报,2009,15(1):114-120.
- [2] Sumfleth K, Duttman R. Prediction of soil property distribution in paddy soil landscape using terrain data and satellite information as indicators [J]. Ecological Indicators, 2008(8):485-501.
- [3] 王凤花,张淑娟.精细农业田间信息采集关键技术的研究进展[J].农业工程学报,2008,39(5):112-121.
- [4] Boonsompopphan Buree, Vearasilp Taweesak, Yos Russell S, et al. Field identification of soil series: in-

dexing and retrieving soil information while sharing experience and knowledge [J]. Field identification of soil series, 2008,173(10):736-744.

- [5] Donoho D L. Denoising by soft-threshold [J]. IEEE Transaction on Information, 1995(3):613-627.
- [6] 文成林.多尺度动态建模理论及其应用[M].北京:科学出版社,2008.

作者简介:



朱培逸 男,博士研究生.研究方向为智能信息处理、智能计算.

孙顺远 男,博士研究生.研究方向为无线传感器网络.

刘柱 男,硕士研究生.研究方向为过程控制.

徐保国 男,博士生导师,教授.研究方向为过程控制及优化.

(上接第17页)

从表2评估结果可知,本文提出的连锁经营企业网络安全评估模型可以网络规模和拓扑发生变化情况下,自动调整相似域的规模来消除网络变化对评估的影响.本文评估模型是一种有效的现代连锁经营企业网络安全评估方法.如果最后考虑连锁经营网络普遍存在的威胁因素(专家调查确定),那么网络安全综合风险值的评估精度会有所提高.

5 结束语

本文针对评估网络环境中实体风险相似性的原理,考虑到实体之间安全关联对整个网络风险的影响,通过将目标评估网络划分为若干个安全相似域进行风险评估,通过应用实例验证本文提出的评估思路是正确的,减少了网络安全计算量,很好的把握住系统安全风险的特点.但是该模型仍有很多问题需要进一步研究,如相似域的合理划分、描述语言的完备性等问题.

参考文献:

- [1] 孙强.基于定量安全风险评估模型的网络安全管理平台[J].微电子学与计算机,2010,27(5):70-73.
- [2] 徐礴晟,张傑穗,李生红.网络安全评估方法研究进展研究[J].信息安全与通信保密,2009(10):50-51.
- [3] 张伟,张宗华,赵霖.一种新型的网络安全策略模型[J].微电子学与计算机,2003,20(4):73-76.
- [4] 汤伟伟,姬敏.现代连锁经营与管理[M].北京:清华大学出版社,2001.
- [5] 邢栩嘉,林闯,蒋屹新.计算机系统脆弱性评估研究[J].计算机学报,2004,27(1):1-11.
- [6] 鲁智勇,冯超,余辉,等.网络安全性定量评估模型研究[J].计算机工程与科学,2009,31(10):100-104.
- [7] 徐源,戴青,郭靓基.基于安全相似域的风险评估模型[J].电子科学技术评论,2005,65(2):200-205.
- [8] 张海霞,连一峰,苏璞睿,等.基于安全状态域的网络评估模型[J].软件学报,2009,28(20):100-120.

作者简介:

蔡京玖 女,(1964—),硕士,讲师.研究方向为计算机网络技术与应用.