DOI: 10.13657/j.cnki.gxkxyxb.2005.s1.034

动态综合信息安全模型及其使用注意事项*

The Dynamic Comprehensive Model of Information Security and Its Points for Attention on

令狐大智[1,2],李陶深[1]

Linghu Dazhi[1,2], Li Taoshen[1]

(1.广西大学计算机与电子信息学院,广西南宁 530004; 2.辽宁工程技术大学电子与信息工程系,辽宁阜新 123000)

(1. School of Comp., Electronics and Info., Guangxi Univ., Nanning, Guangxi 530004, China; 2. Dept. of Electron and Info. Engi., Liaoning Tech. Univ., Fuxin, Liaoning 123000, China)

摘要:在现有信息安全体系模型的基础上提出一种新的信息安全模型——动态综合信息安全模型。该模型综合了其它模型的优点,可以用于指导企业合理、有效地利用各种现有的技术和非技术因素,建立可靠的安全防护体系,提高企业资源的安全性和抗风险能力,它适合于安全防护工程的整个过程,尤其是大型的、复杂的项目。

关键词:信息安全 模型 结构 注意事项 动态

中图法分类号:TP309.2 文献标识码:A 文章编号:1002-7378(2005)S0-0100-03

Abstract This paper brings forward a new information security model-dynamic comprehensive security model based on existing models. This model synthesizes all other models´advantages and makes up their disadvantages. It can help to organize all the present technical and non-technical factors rationally and effectively, so it can help to strengthen enterprises´security structure. This model fits the whole process of security projects, especially those large and complicated ones.

Key words information security, model, structure, points for attention on, dynamic

在当今信息时代,信息安全事件层出不断,给国家、社会和企业造成了重大经济损失和恶劣的影响[1]。信息安全保护工作已成为当前政府、企业信息化进程中的重中之重。

现有安全体系模型主要有 PPDR安全模型、NSTISSC信息安全模型和层次化安全模型[2~4]。这些信息安全模型的使用使信息的安全性得到了一定的保障,但是这些模型都还存在一些不足,没有考虑人的因素,缺少相应的评估等。

对多种已发生的安全事件的调查发现[5],由于人为因素的灵活性及不可测度性,使其在信息安全风险因素中占有重要的位置。因此,要保护信息及其相关系统,仅靠技术是不够的,它还需要政策、培训和教育等手段。由于各种破坏手段的层出不穷,安全防护需求的调整以及信息技术平台本身的脆弱性,使信息安全成为随技术发展、用户需求和各种风险因素推动下不断前进的一门学科。本文在现有信息安全模型的基础上提出一种新的信息安全模型——动态综合信息安全模型。该模型是综合其他模型的优点,修正其缺点而形成的一个安全框架,在特定的情况下,其它模型都是本模型的特例。

1 动态综合信息安全模型

动态综合信息安全模型如图 1所示,模型每次循环都是以鉴别开始。在图 1中的射线状内容表明在完成每一步的累积消耗,蛇形形状表明在完成这个动态模型每一步。动态综合信息安全模型将风险驱动、安全防护策略、安全架构、安全技术、信息安全综合响应平台、人尤其是高层管理人员、安全防护制

收稿日期:2005-09-09

作者简介:令狐大智(1979-),男,山西人,助教,硕士研究生,主要从事网络计算和信息安全领域的研究。

* 广西留学回国人员科学基金项目(桂科回 0342001)和广西科技攻关项目(桂科攻 0385001)联合资助。

度和评估有机组合、协调组成一个动态的螺旋式上升的过程。

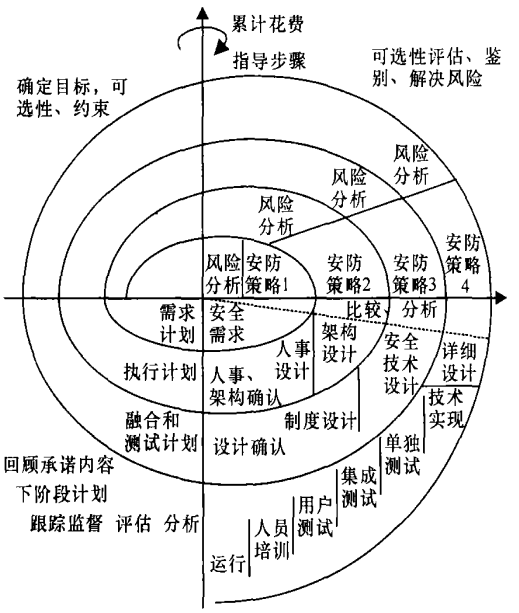

图 1 动态综合信息安全模型

风险驱动,就是在每次上升之前,对当前的安全状况进行风险评估,通过发现的风险来推动和促进安全工作的进行。风险管理评估的结果即制定信息安全策略。

安全策略是用于决定哪些方面是安全防护的重点,哪些资源需要重点防护,并据此制定详实的安全实施计划。

信息安全架构是在风险评估和制定好的信息安全策略的基础上建立的信息安全综合框架。它是从全局安全的角度出发,指出各种安全技术所处的角色和位置以及它们之间如何相互协作和组合,它是构建信息安全平台的模板。

安全防护制度是在安全策略的基础上充分考虑人的因素进而制定的各种规章制度。它是一套用于从整体上规范企业内部人员和外部协作伙伴等在网络、信息使用上所应遵循的措施,并对他们给予指导,用以保证安全防护体系行之有效。图2给出了安全防护制度在使用过程中应遵循的措施,它表示的是一个螺旋式不断上升的过程。

制定安全防护策略和安全防护制度之后,就需要考虑为满足这些目标而要采用的技术以及它们间的关系。由于信息网络的发展和网络、计算机技术本身的弱点,使信息安全隐患存在于信息网络的很多位置[4],任何一个位置保护的不足都会严重损害安全防护系统的整体效果[6]。所以,在选择安全技术时,需要综合考虑各方面因素,在各种技术间取得平衡,有策略的布置防护系统,真正地提高信息安全的防护水平。建议采用层次化的安全防护系统或纵深防御体系,它们把保护措施分层处理,不同层面实现不同功能,这样即使某个层次被突破了,它仍能留下足够的时间对其进行响应,使风险降至最低。

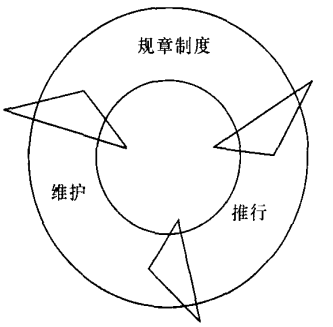

图 2 安全防护制度遵循的措施

目前的攻击手段已经融合了多种技术[7],这就要求各层安全防护产品能相互协作、信息共享,以便共同防御恶意攻击。信息安全综合响应平台就是为了满足层次化防御所采取的综合管理措施,它主要采取信息存储格式标准化、信息传递格式标准化、接口标准化和信息上报机制等用于提高综合响应能力,它可将各处的信息进行汇总,协调各种技术更好的检测攻击。

安全策略、安全制度是信息安全的基础,而人则是它的第二重要因素。一般说来,在任何安全防护体系中,人都是最薄弱的环节[5]。这需要一个合理、有效的安全防护制度让员工来遵守,同时也要对用户行为进行监督和管理。

因此,要得到较好的安全保障,必须要使这些因素相互协调起来,进行联动。

2 动态综合信息安全模型使用中应注意的事项

(1)安全防护是一个持续的过程。安全的实现建立在对现有威胁持续发现的基础上,同时它严重依赖现有的安全技术水平、企业现有的投资水平以及员工的知识层次。因此需要安全防护工作人员时刻关注信息安全技术的发展和各种新型安全威胁的产生,根据企业的发展向管理高层提出新的安全防护建议,所以在使用本模型时要注意到它是一个螺旋式动态上升的过程。每一步完成后都需要进行评估和确认,保证其能达到规定的防护要求。

(2)成本效益问题。尽管安全防护问题很重要,加强防护措施的技术也很多,但安全防护及安全防

护技术不应该成为一个负担,不应该凌驾于它们将要保护的商业利益和原则之上。如果安全防护措施本身比它所保护内容的成本还高,这样的解决方案就需要重新评估。

(3)注意各种技术之间的协同,以及发生安全事件后的应急补救措施。

(4)预防第一。虽然采用各种技术、方法来保护信息安全,但并不可能完全确保安全事件不发生,因此需要事先做好发生各类安全事件的应急措施,以备万一。

安全的实现需要拥有良好的安全防护意识环境。安全防护方面教育和奖励比较自觉和警惕的员工是营造安全防护意识环境的好办法。此外,管理层的支持和参与对安全防护制度的制定和实施有很大的影响,领导应该是遵守安全防护制度的榜样。

3 结束语

动态综合信息安全模型和其它模型相比,最重要的特点是风险驱动和动态综合相平衡,它综合了其它模型的优点,并弥补了它们的缺陷。该模型可以用于指导企业合理、有效地利用各种现有的技术和非技术因素,建立可靠的安全防护体系,提高企业资源的安全性和抗风险能力,它适合于安全防护工程的整个过程,尤其是大型、复杂的项目。

安全防护不是一件孤立的事情,它是根据业务方向和所处环境而持续进行检查和改进的过程。它是人、策略和技术三者之间相互作用的最高点。使用安全防护产品并不是一劳永逸的事情。随着环境的变化,这些产品也必须接受评估和重新配置。同时它需要依靠专业人员的经验来使用,它需要在合同、规范、评估、行程安排和风险分析部分做进一步的描述,以适应安全防护工程的所有情况。

参考文献:

[1] 中国互联网络信息中心.中国互联网络发展状况统计报告[EB/OL]. http://www.cnnic.net.cn/html/dir/2005/01/15/2080.htm, 2005-01-15.

[2] Glen Bruce, Rob Dempsy. Security in Distributed Computing[M].北京:机械工业出版社, 2003.

[3] Joel Scambray, Stuart Mcclure, George Kurtz. Hadking Exposed: Network Security Secrets and Solutions[M]. SAMS, 2002.

[4] Mandy Andress. Surviving Security: How to Integrate People, Process and Technology[M].北京:机械工业出版社, 2002.

[5] CN-CERT/CC, 2004年全国网络安全状况调查报告[EB/OL]. http://www.cert.org.cn, 2004.

[6] Benjurry.木桶新理论与信息安全[EB/OL]. http://benjurry_at_xfocus.org, 2004-06.

[7] 徐 慧,刘凤玉.多特征融合的入侵检测[J].计算机工程, 2004, 30(8): 103-105.

(责任编辑:韦廷宗)