信息网络动态安全体系模型综述

张庆华
(同济大学 经济与管理学院, 上海 200092)

摘　要: 阐述了当前应用较广泛的几个信息网络动态安全体系模型, 指出安全是一个动态的过程, 对安全问题的解决要有一个整体框架, 并体现其动态性。

关键词: 信息安全; 网络安全; 动态安全体系模型
中图法分类号: TP393　　文献标识码: A　　文章编号: 1001-3695(2002)10-0005-03

An Overview of Information and Network Dynamic Security Framework Model

ZHANG Qing-hua
(*School of Economics & Management, Tongji University, Shanghai* 200092, *China*)

Abstract: This paper elaborates some models of information and network dynamic security framework which applied extensively in present. Security is a dynamic process, the solution for security problems should be a total and dynamic solution.

Key words: Information Security; Network Security; Dynamic Security Model

传统的安全防护方法是: 对网络进行风险分析, 制定相应的安全策略, 采取一种或多种安全技术作为防护措施。这种安全方案要取得成功依赖于系统正确的设置和完善的防御手段, 并且在很大程度上针对固定的威胁和环境弱点。这种方式忽略了 Internet 安全的重要特征, 即 Internet 安全没有标准的过程和方法, 所谓"道高一尺, 魔高一丈", 它是矛与盾的无限循环, 安全不是一朝之事, 幻想一劳永逸的解决方案是非常危险的, 新的安全问题的出现需要新的技术和手段来解决; 因此, 安全是一个动态的、不断完善的过程。这就引出了 Internet 安全的新概念——网络动态安全体系模型。

1　基于时间的 PDR 模型

PDR 是防护(Protection)、检测(Detection)、反应(Reaction)的缩写。在 PDR 模型中, 采用 Pt 表示攻击所需时间, 主要是人为的从攻击开始到攻击成功的时间, 也可是故障或非人为因素破坏从发生到造成影响生产的时间; 采用 Dt 表示检测系统安全的时间; 采用 Rt 表示对安全事件的反应时间, 即从检测到漏洞或攻击触发反应程序到具体抗击措施实施的时间。显然, 由于主观不可能完全取消攻击或遭受破坏的原因, 客观无论从理论或实践上不可能杜绝事故或完全阻止入侵; 因此只能尽量延长 Pt 值, 为检测和反应留有足够时间, 或者尽量减少 Dt 和 Rt 值。

当 Pt > Dt + Rt 时系统是安全的; 如果 Pt < Dt + Rt, 则系统是不安全的, 这时有 Et = (Dt + Rt) - Pt, Et > 0 称为暴露时间, 应使其尽量小。

2　P2DR 模型

可适应网络安全理论(或称动态信息安全理论)的主要模型是 P2DR 模型。P2DR 模型是在整体的安全策略的控制和指导下, 在综合运用防护工具(如防火墙、操作系统身份认证、加密等)的同时, 利用检测工具(如漏洞评估、入侵检测等)了解和评估系统的安全状态, 通过适当的反应将系统调整到"最安全"和"风险最低"的状态。

P2DR 模型包括四个主要部分: Policy(安全策略)、Protection(防护)、Detection(检测)和 Response(响应)。防护、检测和响应组成了一个完整的、动态的安全循环, 在安全策略的指导下保证信息系统的安全, 如图 1 所示。

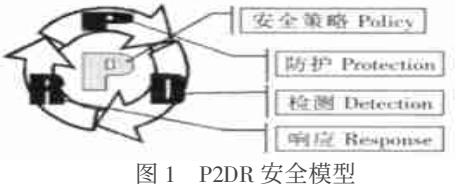

图 1　P2DR 安全模型

在 P2DR 模型的指导下, 用户可以选择更加切合实际的安全解决方案。

信息安全问题十分复杂, 但是作为用户, 面对信息安全归结起来应抓好两件事情:

- 管理原则

实际上就是人的问题, 任何安全问题都涉及到人, 所有的技术、过程都仅仅是表象。安全管理的另一个重要方面就是安全策略。

- 工具原则

工具是人具体实现安全的手段, 是落实安全策略的保证。工具问题包含安全技术, 但是用户不要过分关心

收稿日期: 2002-01-15; 修返日期: 2002-05-08

安全技术本身,因为安全技术太复杂。如何将最新的安全技术转化为产品(工具)应当由安全专业公司来实现。

3 动态自适应安全模型

动态自适应安全模型的设计思想是将安全管理看作一个动态的过程,安全策略应适应网络的动态性。动态自适应网络安全管理模型通过不断地监视网络、发现威胁和弱点来实行安全措施,它给用户一个循环反馈以便及时地作出有效的安全策略和响应。

动态自适应安全模型由下列过程的不断循环构成:安全分析与配置、实时监测、报警响应、审计评估。

3.1 安全分析与配置

模型强调在构建系统时,从一开始就要从整体上考虑系统的安全性。这包括以下内容:标志和认证、存取控制、密码技术、完整性控制、审计和恢复、操作系统安全、数据库系统安全、防火墙系统安全、计算机病毒防护和抗抵赖协议等等。安全分析与配置阶段就是要全盘考虑上述问题,给出相应配置。

3.2 实时监测

实时监测网络攻击模式和其它网络可疑活动,这包括:

①分析黑客行为、病毒特征、系统弱点,提取出数据特征,作为实时监测的知识库和方法库,以便实时监测网络攻击和病毒模式,及时发现系统弱点和漏洞。

②通过对各种网络服务和应用协议的分析,找到各类服务的正常数据流格式和应用方法,作为系统可疑行为知识库,以便实时监测可疑的网络和系统操作。

③根据系统安全规则,建立系统违规行为分析知识库,实时识别网络和系统违规行为。

3.3 报警响应

对发现的各类攻击模式、系统弱点和漏洞、病毒、违规行为、泄密等各种威胁,系统给予相应的响应,包括:

①记录相关信息的日志;

②通过控制台消息、E-mail、页面调度程序发出警告;

③阻断非法连接;

④调用用户自定义的策略程序;

⑤上述这些响应的组合。

3.4 审计评估

审计评估的目的是根据网络的报警记录、日志信息及其它信息向管理员提供各种能够反映网络使用情况、网络上的可疑迹象、网络中发生的问题等有价值的统计和分析信息,运用统计方法学和审计评估机制给出智能化审计报告及趋向报告,综合评估网络安全现状,并把它作为下一次循环的输入状态。

这里要特别强调两点:第一,上述模型中每一个子过程都有可能反馈。因为,在每一过程的检验和确认阶段都可能发现问题,只有不断反馈才能达到理想状况。图 2 表示了该过程。第二,上述模型的整个过程不断循环,形成一个螺旋链式结构。只有这样,Internet 安全才能不断达到新的台阶。可以说,螺旋式前进是信息安全发展的永恒规律。它非常类似总体质量管理方法(Total Quality Management, TQM)。动态自适应安全模型各过程与 TQM 的各步骤对应关系如图 3 所示。

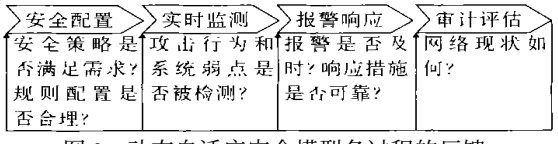

图 2 动态自适应安全模型各过程的反馈

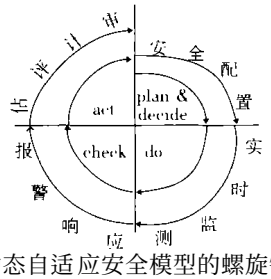

图 3 动态自适应安全模型的螺旋链式结构

4 全网动态安全体系 APPDRR 模型

全网动态安全体系可由下面的公式概括:

网络安全= 风险分析+制定策略+防御系统+实时监测+实时响应+灾难恢复

即网络的安全是一个“APPDRR”的动态安全模型,如图 4 所示。

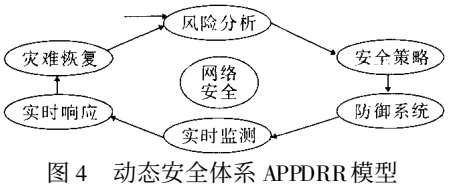

图 4 动态安全体系 APPDRR 模型

从安全体系的可实施、动态性角度,动态安全体系的设计充分考虑到风险评估、安全策略的制定、防御系统、监控与检测、响应与恢复等各个方面,并且考虑到各个部分之间的动态关系与依赖性。

进行风险评估和提出安全需求是制定网络安全策略的依据。风险分析(又称为风险评估、风险管理),是指确定网络资产的安全威胁和脆弱性,并估计可能由此造成的损失或影响的过程。风险分析有两种基本方法:定性分析和定量分析。在制定网络安全策略的时候,要从全局进行考虑,基于风险分析的结果进行决策,建议公司究竟是加大投入,采取更强有力的保护措施,还是容忍一些小的损失而不采取措施。因此,采取科学的风险分析方法对公司的网络进行风险分析是非常关键的。

一旦确定有关的安全需求,下一步应是制定及实施安全策略,以保证把风险控制在可接受的范围之内。安全策略的制定,可以依据相关的国内外标准或行业标准,也可以自己设计。有很多方法可以用于制定安全策略,但是,并不是每一组安全策略都适用于每个信息系统或环境,或是所有类型的企业。安全策略的制定,要针对不同的网络应用、不同的安全环境、不同的安全目标而量身定制,各公司应该按照自己的要求,选择合适的安全体系规划网络的安全。制定自己的安全策略应考虑以下三点内容:①评估风险;②企业与合作伙伴、供应商及服务提供商共同遵守的法律、法令、规章及合约

条文;③企业为网络安全运作所订立的原则、目标及信息处理的规定。

图 4 的安全模型为网络建立了四道防线:安全保护是网络的第一道防线,能够阻止对网络的入侵和危害;安全监测是网络的第二道防线,可以及时发现入侵和破坏;实时响应是网络的第三道防线,当攻击发生时维持网络"打不垮";恢复是第四道防线,使网络在遭受攻击后能以最快的速度"起死回生",最大程度上降低安全事件带来的损失。

安全管理贯穿在安全的各个层次实施。实践一再告诉人们,仅有安全技术防范,而无严格的安全管理体系相配套,是难以保障网络系统安全的;必须制定一系列安全管理制度,对安全技术和安全设施进行管理。从全局管理角度来看,要制定全局的安全管理策略;从技术管理角度来看,要实现安全的配置和管理;从人员管理角度来看,要实现统一的用户角色划分策略,制定一系列的管理规范。实现安全管理应遵循以下几个原则:可操作性原则;全局性原则;动态性原则;管理与技术的有机结合;责权分明原则;分权制约原则;安全管理的制度化。

5　信息安全保障体系 IA 与 WPDRRC 模型

美国国防部对信息保障 IA(Information Assurance)作的定义是:"通过确保信息/信息系统的可用性、完整性、可验证性、机密性和不可抵赖性来保障信息/信息系统的安全。"

信息保障的内涵已超出传统的信息安全保密,而是防护(Protection)、检测(Detection)、反应(Reaction)、恢复(Restore)的有机结合,称之为 PDRR 模型,如图 5 所示。

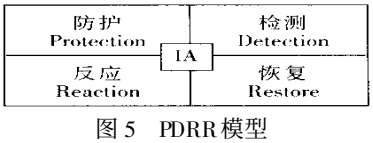

图 5　PDRR 模型

IA 认为仅仅依靠政策、法规和加密技术是不够的,还必须建立一个实体来操作。在美国的带动下,一些信息技术发达国家相继在政府、军队、大学、科研单位、企业部门成立了专门处理计算机安全事件的机构,其名称一般沿用美国率先采用的"计算机紧急事件响应工作组(CERT)"。他们不仅负责本部门管辖的计算机安全事宜,而且还互通信息,密切合作。特别是美国发起成立了国际性"计算机紧急事件响应与安全工作组论坛(FIRST)",成员数目增加很快。我国已经成立了国家计算机网络应急处理协调中心 CNCERT。该中心是在国家因特网应急小组协调办公室的直接领导下,协调全国范围内计算机安全事件响应小组(CSIRT)的工作,以及与国际计算机安全组织的交流。CNCERT 还是负责为国家重要部门和国家计算机网络应急处理体系的成员提供计算机网络应急处理服务和技术支持的组织。目前,CNCERT 正准备加入 FIRST。

IA 不仅是一个技术问题,也是一个管理问题。在一个组织内部,复杂性和风险性随组织级别的增加而增加。因此,IA 一定要从组织管理的角度来审视和对待。实际上,在组织管理的最高级别,复杂性和风险性也是最大的,所以,IA 的技术解决方案应当由组织管理解决方案来驱动。通常,IA 的管理工作要从三个方面来考虑:计划管理、风险管理和培训教育。需要强调的是计划管理,通过计划管理可以减少导致计划失败的可能因素,形成一个从策略、流程、技术方案和管理勘漏多个方面综合考虑的管理框架。

实施 IA 是复杂和有风险的,需要在一个极其不稳定和变化的环境中操作,因此,有必要考虑一些关键因素:①要确保高层领导给予高度重视和资金保障;②要透彻理解 IA 计划的复杂性;③要把 IA 计划作为一个独立项目启动,如果仅被视为另一个计划的扩展和延伸,会导致资源的紧张;④要规划并测试实施策略,以避免投入了时间和资源却设计了一个未能符合实施要求的策略;⑤要制定流程以方便和确保足够的内部信息沟通和有效交流;⑥要整合关键流程,这样当计划发生改变时,其对整个流程产生的影响会马上显现出来;⑦要有可量度的控制工具即标准,结论。

我国需要适合国情的科学的信息安全保障体系结构,可用 WPDRRC 来反映六大能力和三大要素:①六大能力——预警能力、保护能力、检测能力、反应能力、恢复能力、反击能力。②三大要素——人、政策、技术。信息安全保障框架模型如图 6 所示。

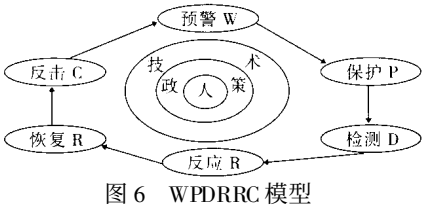

图 6　WPDRRC 模型

6　结束语

无论从时间,还是从现有的知识水平来看,我们都不可能从一开始就能将安全问题及其相应的解决方案考虑得滴水不漏。安全是动态的,它随着新技术的不断发展而发展;它是一个集技术、管理、法律法规和标准综合作用为一体的系统工程,因此对安全问题的解决要有一个整体框架,并体现其动态性。

参考文献:

[1] 康勇建,姚京松,林鹏. 基于 PDR 模型的银行计算机网络动态适应安全系统[J]. 中国金融电脑,2001,13(2):73-75.

[2] 潘宇东. P2DR 模型——网络安全管理的指南[J]. 微电脑世界,2001,16(20):3-5.

[3] 陈洪波. 如何实现动态网络安全[J]. 信息网络安全,2001,1(2):15-20.

[4] 沈昌祥. 浅谈信息安全保障体系[J]. 信息网络安全,2001,1(1):16-28.

[5] 姜朋. 信息安全与 IA 计划[J]. 信息网络安全,2001,1(4):43-44.

[6] 赵战生. 我国信息安全保障体系结构框架的构想[C]. 上海:2001 年上海首届信息网络安全高层论坛发言,2001.

作者简介:

张庆华(1977-),女,同济大学经济与管理学院管理科学与工程专业博士生,研究方向为信息安全管理。