文章编号:1002-980X(2007)10-0125-04

网络经济安全技术体系解析

关国华

(浙江大学 理学院, 杭州 310028)

摘要:在网络经济时代,信息安全至关重要,随着我们对信息安全认识的逐步深入,如信息保障技术框架(IATF)、信息安全管理体系(ISMS)、信息系统安全工程(ISSE)、风险分析(RA)以及新近出现的等级保护、可信计算等等。在未来的信息安全领域,除了我们对已有的安全设备和安全系统进一步从性能、功能、易用性方面进行提升外,一个很重要的任务就是在安全系统的运行管理方面提供可信的安全管理,实现系统的安全可靠运行,确保网络发挥其经济和社会效益。

关键词: 网络安全;安全体系

中图分类号:TN915.08 **文献标志码**:A

随着信息网络的不断发展,其巨大的社会和经济效益越来越受大众的关注,信息传输通道全面转向语音、数据、多媒体、视频、电子政务、电子商务等多元化的综合业务网络平台,特别是在电子政务网络建设中,如何有效化解安全风险,如何应对各种突发性安全事件已成为紧迫的问题摆在我们面前。在1998年以前,谈到信息安全时可能首先想到的是信道安全、邮件加密等内容;1998年以后,经过了几年的发展,目前出现种类颇多的信息安全产品,如防火墙、漏洞扫描、入侵检测、Ipsec VPN/SSL VPN、邮件过滤系统、病毒蠕虫防护系统、内容安全网关、单点登录系统、证书管理系统等等,并且形成了许多典型解决方案。我们对信息安全的认识也在逐步深入,在此过程中我们历经了多种理念的洗礼,如信息保障技术框架(IATF)、信息安全管理体系(ISMS)、信息系统安全工程(ISSE)、风险分析(RA)以及新近出现的等级保护、可信计算等等。当一个系统没有安全设备时,我们认为它一定不安全;但部署了上述种类繁多、配置管理复杂的安全设备后,系统的安全性又如何,系统中的安全设备运转状态以及其发挥的效用、对系统中的网络安全事件是否就心中有数了?作者认为,在未来的信息安全领域,除了我们对已有的安全设备和安全系统进一步从性能、功能、易用性方面进行提升外,一个很重要的任务就是在安全系统的运行管理方面提供可信的安全管理,实现系统的安全可靠运行。

本文重点讨论实现可信管理所需要的重要设施安全运行维护中心/安全运行中心(SOC:security operation center)的原理和实现。SOC是对传统安全管理方式的一次变革,它充分利用空间、时间、知识、能力等诸要素,构建综合预警、应急响应的体系,为全面管理信息系统提供基本保障。作者认为这是一个大有发展前景的研发方向,具有极大的商业价值,也是一个需要深入探索和研究的领域。

1 SOC的模块组成分析

随着信息化建设步伐的加快,如何有效化解安全风险,有效应对各种突发性安全事件已成为不容忽视的问题。特别是对于地域分散、规模庞大的系统,如何将现有安全系统纳入统一的管理平台,实现安全形势全局分析和动态监控已成为各级信息系统维护部门面临的主要问题,SOC就应运而生。SOC通过集中收集、过滤、关联分析安全事件,提供安全趋势报告,及时做出反应,实现对风险的有效控制,参见图1。SOC主要包括事件发生模块E Box、事件收集模块C Box、归一化事件存储模块D Box、事件分析模块A Box、(需要利用知识库模块K Box)、事件反应模块R Box,下面分别将这些模块说明如下。

1.1 事件发生模块(E Box)

事件发生模块负责生成安全事件,可分为两类:一类是基于数据的事件发生模块,一类是基于状态

收稿日期:2007—04—28

作者简介:关国华(1969—),男,广东广州人,浙江大学博士生,主要从事人力资源和电子政务研究。

的事件发生模块。前者指传感器,如网络入侵检测系统、主机检测系统、防火墙等,主要产生由操作系统、应用和网络操作等引发的事件;后者指轮询器,产生响应外部激励(如 Ping、SNMP 命令)的事件,外部激励主要用来检查服务状态和数据完整性等,这类事件的典型例子是网管系统中轮询工作站向管理工作站发送的告警信息。安全事件主要由传感器产生,最典型的传感器是入侵检测系统,但也可以是任何具备日志功能的过滤系统,如防火墙、具备访问控制列表功能的路由器、具备 MAC 地址过滤功能的交换机等,也可以是 Sniffer 等网络监听设备或蜜罐系统。

1.2 事件收集模块(C Box)

事件收集模块负责从不同传感器收集信息并转换为标准格式,从而形成统一信息以方便后续的处理。在事件收集过程中,出于安全性考虑,往往需要采用加、解密技术保证消息的机密性和完整性,从而实现了对系统的安全和可信的管理。

1.3 事件存储模块(D Box)

可以将事件存储模块简单理解为数据库,只是它需要进行相关性处理,要识别来自同一源或不同源的重复事件。

1.4 事件分析模块 + 知识库(A Box + K Box)

分析存储在数据库中的事件,为事件响应模块提供响应的充分依据,在具体分析过程中,离不开知识库(K 模块)的支持,知识库存储入侵路径,系统安全模型、安全策略等知识。分析模块包括相关性分析、结构化分析、入侵路径分析及行为分析等,是 SOC 系统最复杂的部分。

1.5 事件响应模块(R Box)

响应模块功能负责对安全事件做出及时有效响应,涵盖反击正在发生安全事件的所有响应和报告工具。由于牵扯到人的因素,响应行为具有相当的主观性,很多时候需要根据长期积累的基于经验的最佳实践(Best Practice)或建议。事件响应模块不仅需要对外提供自动化的控制台接口、事件快速响应接口、实时监控接口、统计分析接口;还需向用户提供永久性的风险评估报告、中长期安全行为报告和系统状态报告等。除了需要安全子系统及时报告安全事件,SOC 对安全事件的响应常常也借助于安全系统,例如防火墙与入侵检测系统联动,在防火墙中动态添加过滤规则。

在 P2PDR(Risk analysiss、Policy、Protection、Detection、Response)模型,而 SOC 系统除了实现其中的 D(Detection)和 R(Response)外,加强了一体化管理功能。

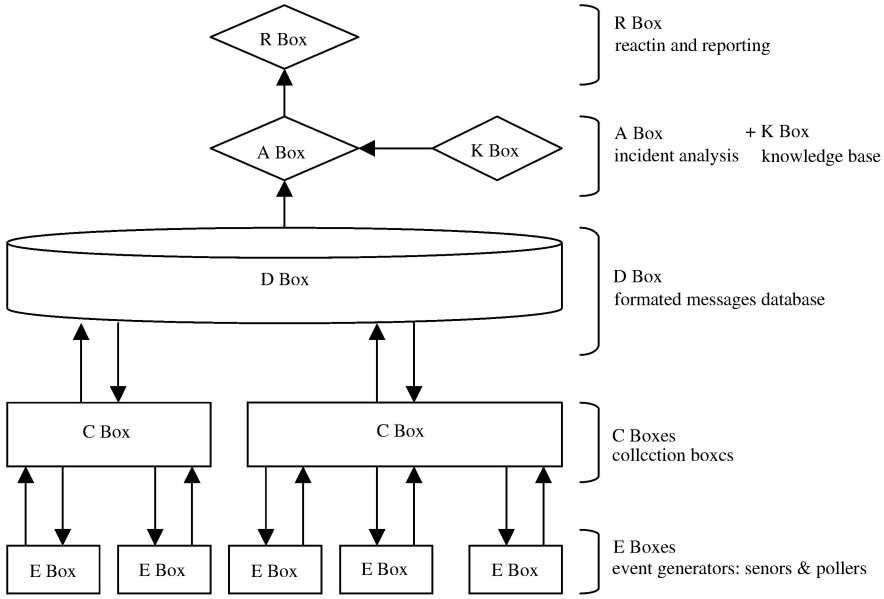

图 1 SOC 的模块组成示意图

SOC 的管理范围包括:网络系统的安全;应用系统的安全;所有网络和系统用户的管理;所有安全产品组成的安全体系的实时管理和监控;所有非安全产品的关键应用系统均应该通过一定途径将安全相关信息输送到安全管理中心中,保证对安全事件的及时发现、分析和响应;负责协助管理层制定和实施长期安全目标和策略;负责日常安全配置和维护。

2 SOC 关键模块功能分析

下面我们重点讨论一下 A Box 中的事件收集和存储,A Box 和 K Box 中的脆弱性数据库以及相关性分析等方面的内容。

2.1 事件收集和存储

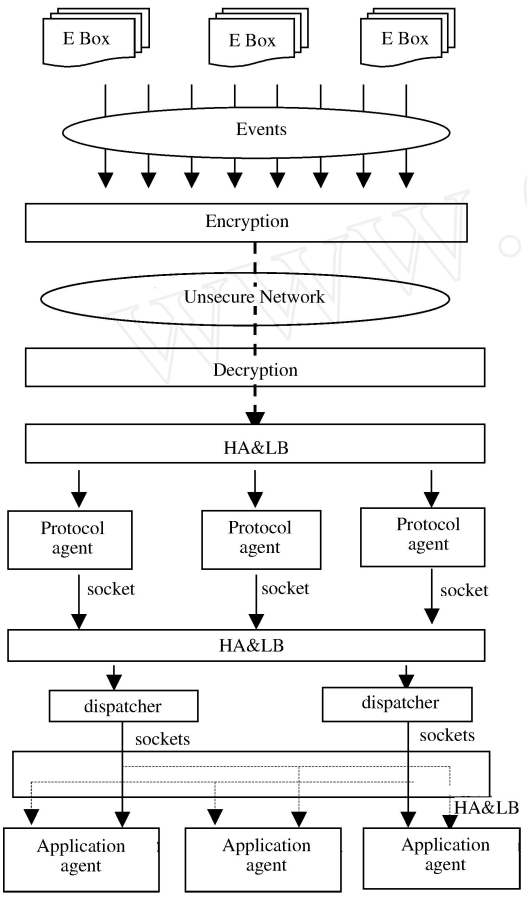

图 2 分布式环境下 SOC 中事件收集示意图

图 2 示例了分布式环境下数据收集,图 3 示例了为本地环境中的数据收集。可以看出,为了实现数据收集,需要很多协议代理,为了保证在分布式环境中处理的性能,需要考虑 HA(High Availability)&LB(Load Balance),需要考虑消息的安全性。在数据的存储方面,需要充分考虑数据的管理与维护。

2.2 脆弱性数据库

脆弱性是指系统存在的安全漏洞或不安全的行为,这些信息可能损害整体安全级别,也可能被"黑客"加以利用发动入侵攻击。作为知识库的一个组件,脆弱性数据库存储三类脆弱性:

1)结构化脆弱性,通常指软件的内部缺陷,例如缓冲区溢出 Bug、安符串格式化缺陷等。

2)功能化脆弱性,通常指与配置、操作行为、用户等运行环境有关的弱点,定义、格式化、整理这类脆弱性,需要操作系统、网络、应用各方面专家的参与。

3)拓扑相关脆弱性,它主要基于网络(如监听、IP 欺骗),还包含可能的入侵路径的脆弱性。拓朴相关脆弱性导入弱点数据库一般需要拓朴建模的支持。

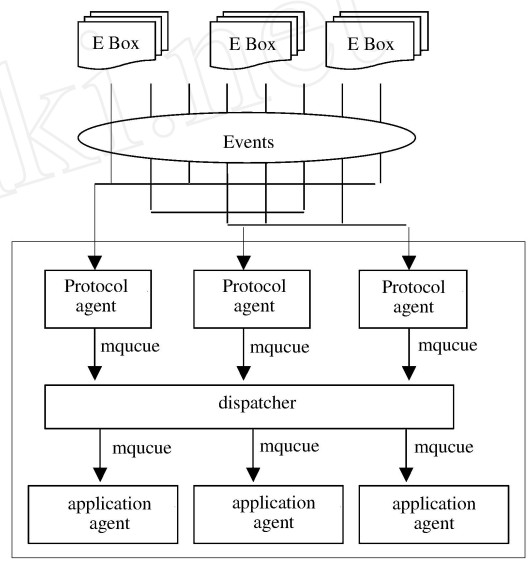

图 3 本地环境 SOC 中事件收集示意

2.3 安全事件的分析

安全事件分析模块综合分析来自不同设备、数量庞大和复杂的事件序列,通过模式匹配找出安全事件之间的内在联系,即相关性,最终产生高度合成的准确分析结果。分析处理的好坏直接关系着 SOC 系统的后续处理。模式分析的基本内容包括:识别重复信息,对于收到的多条重复信息进行筛选/过滤,以减轻存储负担和处理负担;序列模式匹配,判别一系列消息是否由不同入侵企图触发;事件模式匹配,通过基于时间的上下文分析,识别缓慢分布式入侵过程;安全策略匹配,基于行为匹配识别符合安全策略规则的某些事件,如管理员登录、认证;系统威胁分析,判断目标系统是否受已检测到攻击企图的威胁,并分析此类攻击对系统安全的整体影响。

3 SOC 的关键技术

从上面的分析可以看出,在 SOC 建设和实践中,有一系列需要解决的问题,比如效率问题,要在有效提高应用系统安全性的同时,尽量减轻安全事件相关操作对业务系统性能的影响。

我们分析认为需要解决好负载均衡技术、源过滤技术、模式分析等相关性分析技术、结构化分析等脆弱性分析技术、快速响应技术,才能让 SOC 的性

能得到提升,才能很好的发挥共应有的功效。

4 结束语

传统的安全管理方式是将分散在各地、不同类系统就近分别管理,这样导致安全信息互不相通,安全策略难以保持一一对致,不能保证系统整体效益的发挥。SOC 是针对传统管理方式的一次变革,它将关键设备的安全管理集中到一起,最大的优势是为统一安全管理提供了完整平台,从面提高了对于安全威胁的精确检测能力和一体化响应能力,此外我们需要将 SOC 与现有安全管理制度、流程有机衔接才能发挥其功效。SOC 是一个新生事物,国内没有成熟的运维经验,在标准制定、与业务集成等等方面的工作还很多,也需要在发展中不断完善,但它事实上已成为网络运维不可或缺的重要组成部分。

参考文献

[1]仇剑锋,蔡志兴. 信息网络安全设计策略[J]. 大众科技,2006(1):96 - 97.

[2]蔡军红. 浅谈网络信息安全的四个层次[J]. 信息安全,2002(06).

[3]张国锋. 网络信息安全解决方案[J]. 计算机与网络,2002(17).

[4]刘迎风,祁明. 容灾技术及其应用[J]. 计算机应用研究,2002(6):7 - 10.

[5]古利勇,黄元飞,罗万伯. 网络安全运行平台管理体系结构研究[J]. 电信科学,2006(02).

The Analysis of Cybereconomy Security System

GUAN Guo-hua

(Zhejiang University, HangZhou 310028, China)

Abstract: In current cybereconomy time, information security is considerably important. As more and more we know about the information security ——such as Information Assurance Technical Framework (IATF), Information Security Management Specification (ISMS), Information System Security Engineering (ISSE), Risk Analysis (RA), hierarchy protection and reliable Computing, etc., I think in coming information security fields, we should not only enhance capability, function, and convenience of the security equipment and system that we have, but also provide reliable security management, in order to achieve system security and make sure that network can have its economical and social benefits properly.

Key words: network security; security system

(上接第 83 页)

币的稳定性可以通过对银行资产负债表的控制而获得。在银行经营状况较差而不具备抵御风险的能力时,币值的稳定性与银行的清偿力之间则呈现出此消彼涨的关系。这时,政策制定者必须在币值稳定和银行清偿力之间做出选择,该政策选择是一个经济、政治、以及一系列制度的函数。

参考文献

[1]马图. 结构化衍生工具[M]. 林涛,杜育强,王晖,高强,译. 北京:经济科学出版社,2000.

[2]黄俊立,余维彬,张正鑫. 金融工程 ——理论与应用[M]. 武汉:武汉大学出版社,2000.

[3]BUITER W H. Borrowing to defend the exchange rate and the timing and magnitude of speculative Attacks[J]. J. Int. Econ.,1987,23:221 - 239.

[4]GRILLI V. Managing exchange rate crisis: Evidence from the 1980s[J]. J Int. Money Finance,1990,9: 143 - 156.

On the Financing Role of Bank System in Attack of Currency Speculation

CHU Jing-yuan

(Department of Economy, Wuhan University of Technology, Wuhan 430007, China)

Abstract: The financial crisis which broke out in Southeast Asian Nations last century caused heavy loss in these countries even in all over the world. After the crisis, a few scholars studied the relationship between these counties' bank performance and the crisis, which indicated that bank system of poor performance often causes the break out of currency crisis. This paper develops a new study style on the problem, discussing the financing role of good bank system in attack of currency speculation, then suggests that it's necessary to hand national credit amounts.

Key words: speculate; currency crisis; banking