



基于业务流程粒度的安全风险管理的分析及应用

谭 彬

(中国移动通信集团广西有限公司信息安全管理中心 南宁 530022)

摘 要:现有以资产为核心的安全风险模型,不能满足业务风险管理的实际需要。通过建立基于业务流程粒度的安全风险模型,并在 WAP、短信业务系统成功实施和应用,真正实现了基于业务流程粒度的风险管理。安全管理员和业务系统管理员可清晰了解业务系统各个流程环节的安全风险状况,有效聚焦和优先处理业务系统关键业务流程的安全告警和风险;安全主管可基于业务流程感知有针对性地对安全风险态势进行规划、制定和实施安全防护方案,真正满足企业对业务安全风险管理的需要,提高业务安全风险管理水平。

关键词:安全风险模型;业务流程;WAP 系统;短信业务系统

doi: 10.3969/j.issn.1000-0801.2013.11.029

Analysis and Application of Security Risk Management Based on Business Process Granularity

Tan Bin

(Information Security Management Center, China Mobile Group Guangxi Co., Ltd., Nanning 530022, China)

Abstract: Existing assets as the core of the security risk management models, cannot meet the actual needs of business risk management. Through the establishment of security granularity based on business process risk management models, and the realization and application in the WAP, SMS systems, the business risk management was realized. Security administrators and business system administrators can clearly understand the security risk situation of business systems, effectively focus and prioritize critical business systems, business processes and the security alarm; based on perceived security risk posture, security officer may plan, develop and implement safety programs, to improve operational safety risk management.

Key words: security risk management, business process, WAP system, SMS system

1 引言

安全风险模型是信息安全管理工作的核心,安全风险体现了业务面临潜在威胁可能遭受的损失,信息安全管理工作的目标是将损失控制在可知、可量化、可控的范围内,并对无法消除的风险进行紧密监控。同时,安全风险模型将识别并量化潜在损失,作为安全防护措施的实施依据。

安全风险评估采用定量和定性结合的风险分析办法实现对资产的安全风险评估和计算,量化的风险分析方法就是把构成风险的各个要素和潜在损失的水平赋予某种数值,当度量风险的所有要素(资产价值、威胁频率、脆弱性利用程度、安全措施的效率 and 成本等)都被赋值时,风险评估的整个过程和结果就都可以被量化。

传统的安全风险管理模型,以资产为基础,通过对资

产价值、资产脆弱性、安全威胁因素关联后计算资产的风险值,并对资产风险实现动态管理。基于资产的风险管理方式,无法从业务角度,特别是业务流程环节的角度反映业务安全风险的状态,也无法有效定位业务流程中存在风险的环节。通过对电信运营业务流程安全风险的管理分析及应用,实现从业务流程角度对安全风险的分析 and 定位,为降低电信运营业务的安全风险提供有效的技术支撑手段。

2 现有安全风险管理模型

电信运营业务系统安全管理的主要目标是保障信息、信息系统和业务的保密性、完整性和可用性。为达到这个目标,目前主要通过建设安全运营中心(security operations center, SOC)以获得技术和管理的综合安全管理支撑手段。

SOC 系统是以资产为核心,以安全事件管理为关键流程,对资产风险模型进行事件分析、风险分析、预警管理和应急响应处理的集中安全管理系统。SOC 系统是从资产的角度,实时监控 IT 信息资产的事件、脆弱性、设备的各种运行状态等安全信息,根据告警规则分析计算生成告警信息,从而通过监控告警实时掌握全网的信息安全状态。其安全风险分析模型的技术实现方案如下。

(1) 资产模型

资产→业务系统→电信运营商企业

说明:多个资产组成一个业务系统,多个业务系统组成电信运营商的企业 IT 系统。

(2) 风险计算模型

资产风险→业务系统风险→电信运营商企业风险

说明:首先以资产为单位,通过风险计算获得资产个体的风险值;然后对业务系统相关的资产组合进行综合计算,得到业务系统风险;最后由所有业务系统的风险组合计算得到企业的风险,从而得到企业整体的信息安全风险状态。

(3) 安全风险告警方式

根据安全事件等的信息分析结果,以资产为单位产生告警信息,提供实时告警监控和处理机制。

现有安全风险管理模型是从资产的角度进行整网安全告警监控管理,以资产和业务系统的角度进行风险管理。缺点介绍如下:

- 仅支持资产信息和安全设备告警信息的关联;

- 仅支持有安全告警的资产和资产责任人的关联;
- 不支持基于业务流程的安全告警监控和风险分析,从而导致无法识别安全告警对业务系统各个环节的影响程度和危害程度,也无法有效判断处理优先级。

基于上述考虑,设计一种针对电信业务流程和业务安全管理的安全风险管理模型,通过业务流程的粒度分析和电信运营商的网络信息安全风险的管理,实现自动化的电信业务安全管理功能。

3 基于业务流程粒度安全风险管理的设计及实现

本应用设计是在现有 SOC 系统的基础上,实现基于业务流程粒度的安全风险管理,满足业务及其流程的安全风险管理需要。为突出业务及其流程在安全管理系统中的重要性和地位,基于业务流程粒度的安全风险管理系统被称为业务安全管理平台(business security management platform, BSMP)。

BSMP 具有下述功能模块。

- 资产管理模块:提供对业务系统、主机、数据库、网络设备、应用软件等被管对象和安全支撑系统(如入侵检测、防火墙、防病毒、漏洞扫描、终端管理系统等)的资产信息收集和管理。
- 业务流程管理模块:提供业务系统的业务流程和业务节点的定义,提供资产与业务流程节点的关系管理,提供业务流程粒度的安全管理界面展示。
- 事件采集/解析模块:对资产安全事件、漏洞和安全配置脆弱信息、补丁信息进行采集;经过 BSMP 处理,能够将各种资产设备原始的安全事件进行标准化解析,并通过设置过滤规则、归并规则和关联规则筛选出符合规则的安全事件,并与资产关联,生成告警信息。
- 业务安全分析模块:提供业务系统流程节点的风险计算和告警规则配置管理;通过对资产安全事件、漏洞以及配置脆弱点信息的综合风险计算分析,生成基于业务系统流程节点的告警和风险信息。安全风险处理流程如图 1 所示。

下面对 BSMP 的关键设计进行说明。

3.1 基于业务流程粒度的分析风险模型设计

现有的安全风险分析管理都是从设备的粒度分析风险,本设计则是从业务流程的角度分析风险,实现安全风

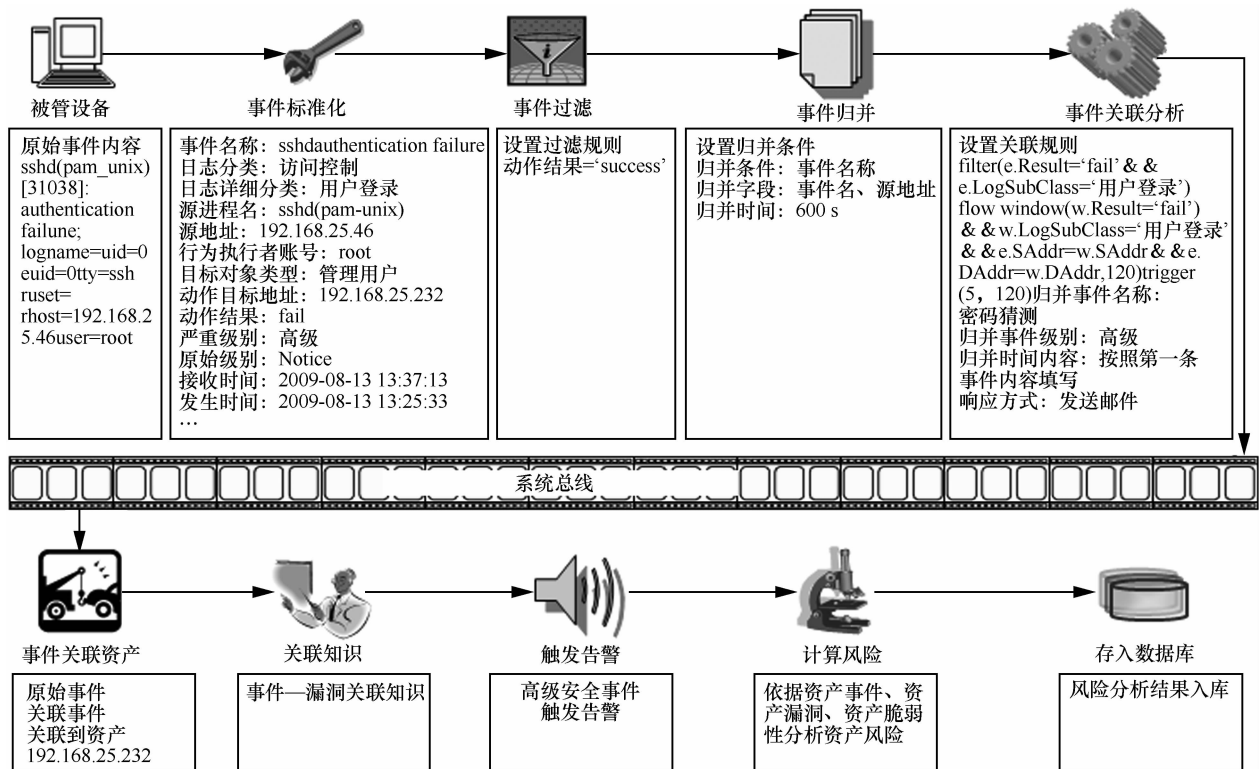


图1 安全风险处理流程示意

险分析关注点从系统设备层面到业务层面的提升,满足对业务层面安全风险管理的需要。

基于业务流程粒度的风险分析模型如图2所示。

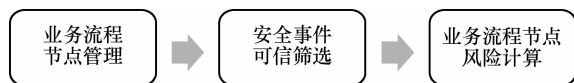


图2 基于业务流程粒度的风险分析模型

通过业务流程节点管理,将资产与业务流程节点进行关联。业务系统流程节点的安全风险来源于该节点所关联的资产,通过对各个业务流程节点相关资产的安全事件、脆弱性(漏洞、安全配置脆弱性)、补丁、端口服务状态等安全信息进行集中采集和综合分析,形成业务节点风险。

3.1.1 业务流程管理设计

业务流程管理实现对业务系统业务流程节点的管理,提供资产与业务流程节点的关系管理,具体如下。

- 业务流程管理: 提供业务系统业务流程的管理,对业务流程名称和描述进行定义,可绘制业务流程图,对业务流程图上的业务流程节点与具体业务节点名称进行关联配置。
- 业务节点与资产关系管理: 提供业务节点与具体业

务资产的关联关系管理。

3.1.2 安全事件可信筛选

由于安全事件量极为庞大,为滤除大量的误报事件信息,提高安全事件的可信度,在进行安全风险分析前,对安全事件进行资产关联分析处理。

安全事件可信筛选是通过把安全事件的源地址、目的地址等属性与资产的系统版本、漏洞、补丁等进行关联,并计算出事件的可信度,从而判断某个安全事件是否能造成不良影响以及造成不良影响的严重程度。

资产可信度筛选规则示例见表1。

3.1.3 基于业务流程粒度风险计算

根据是否基于资产价值,基于业务流程粒度的风险计算模型可以细分为如下两种。

(1) 业务流程粒度安全风险子模型一: 基于资产累计的风险

本风险计算方法是基于业务流程中相关资产的未处理告警计算而来的,某资产风险的计算式为:

$$R = \min(100, \min(100, I_R + \lg(\sum i_R \times i_{ims}))) \quad (1)$$

其中, $\min S$ 表示集合 S 中的最小值, $\lg N$ 表示以 10 为底 N 的对数, I_R 为一个资产最严重的未处理告警风险值, i_R

表 1 资产可信度筛选规则

规则编号	规则描述	匹配内容
1	If [攻击事件目标匹配资产] or [攻击事件源匹配资产] Then [事件可信度增加 M1] Else [事件可信度降低 X1]	资产
2	If [事件目标端口匹配目标资产的端口] Then [事件可信度增加 M2] Else [事件可信度降低 X2]	端口
3	If [事件系统版本匹配目标资产的系统版本] Then [事件可信度增加 M3] Else [事件可信度降低 X3]	系统版本
4	If [目标资产存在事件相关漏洞] or [源资产存在事件相关漏洞] Then [事件可信度增加 M4] Else [事件可信度降低 X4]	漏洞
5	If [目标资产缺乏事件漏洞相关补丁] or [源资产缺乏事件漏洞相关补丁] Then [事件可信度增加 M5] Else [事件可信度降低 X5]	补丁

为一个未处理告警的风险值, i_{times} 表示某未处理告警的累计次数, R 为当前风险值, 取值 0~100。

某业务流程风险的计算式为:

$$\text{某业务流程风险} = \frac{\sum_{i=1}^n (A_i \times R_i)}{\sum_{i=1}^n A_i} = \sum_{i=1}^n \frac{A_i}{\sum_{j=1}^n A_j} \times R_i \quad (2)$$

其中, A_i 和 R_i 分别为各个资产的价值和风险状况。

(2) 业务流程粒度安全风险子模型二: 基于总体告警情况的风险计算模型

本风险计算方法是基于业务流程中所涉及资产的未处理告警计算而来的, 其具体计算式如下:

$$R = \min(100, \min(100, I_R + \lg(\sum i_R \times i_{times}))) \quad (3)$$

符号定义基本同上。 I_R 代表整个业务流程中所涉及资产报出的未处理告警的最高风险值, 而 i_R 为业务流程中涉及的所有未处理告警的风险值。

从上述两个模型可以看出, 两者的唯一差别在于: 前者会将资产价值计算在内, 而后者不会。两者计算出的风险值会存在较大差异, 一般后者会大于前者。在实际应用中, 一般采用子模型一。

3.2 基于业务流程粒度安全风险展示设计

业务系统的整个流程和流程节点以图形方式进行展示, 实时动态展示各个业务流程节点的风险状态。当某个节点存在风险时, 将根据风险的严重程度以不同的颜色显示相应的业务节点。用户点击某个业务节点后, 可以钻取查看具体告警信息, 并对告警进行处理操作。

无线应用协议(wireless application protocol, WAP)业务流程风险状态监控界面如图 3 所示。

每个业务流程的节点一旦有风险告警产生, 则会通过红、橙、黄、绿 4 种颜色代表其业务流程节点的告警级别(绿色表示无风险), 并按照如下规则显示:

- 在该节点下如果有任意数量的高风险告警, 则此节点为高风险节点, 显示为红色;

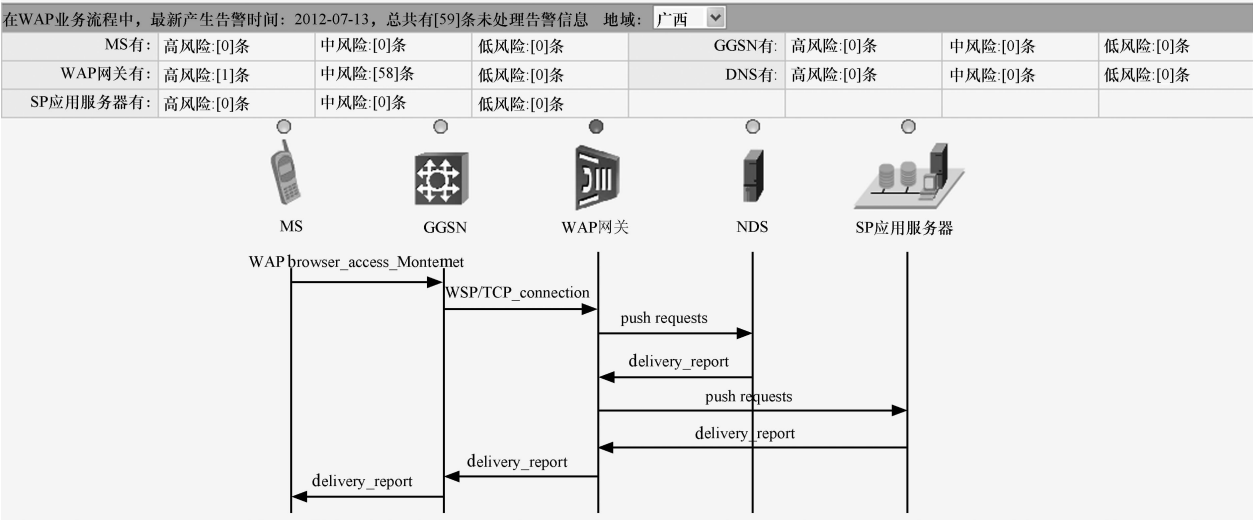


图 3 WAP 业务流程监控管理示意

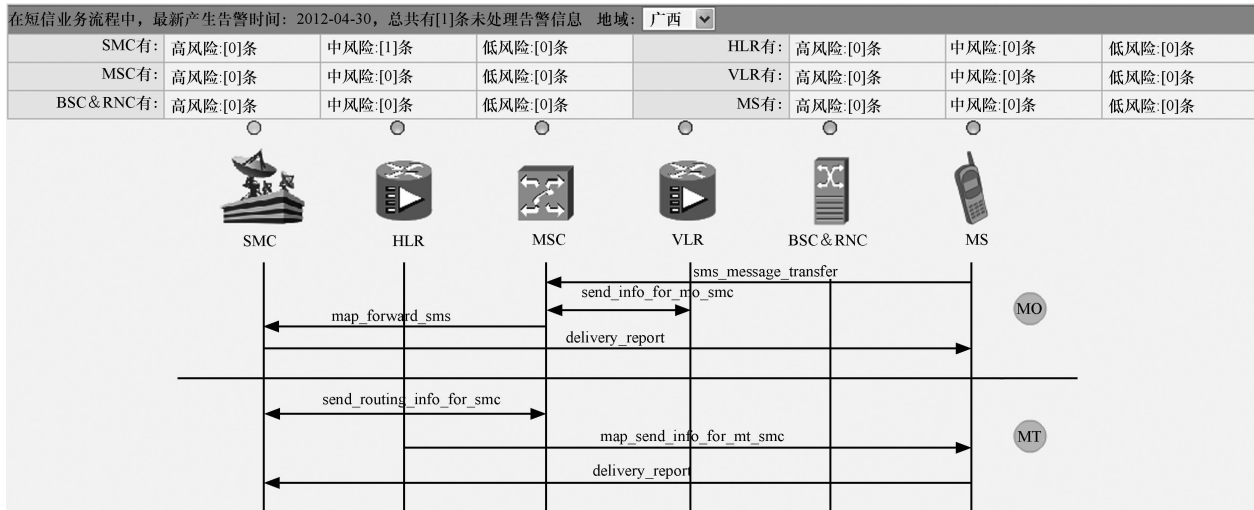


图4 短信业务流程监控管理示意

- 在该节点下无高风险告警,中风险告警数量大于资产总数量的 1/3,则此节点为高风险节点,显示为红色;
- 在该节点下无高风险告警,中风险告警数量小于资产总数量的 1/3,则此节点为中风险节点,显示为黄色(忽略低风险告警数量);
- 在该节点下无中高风险告警,只要低风险告警数量大于资产总数量的 2/3,则此节点为中风险节点,显示为黄色;
- 在该节点下无中高风险告警,只要低风险告警数量小于资产总数量的 2/3,则此节点为低风险节点,显示为绿色。

3.3 基于业务流程的告警处理

通过业务流程节点安全风险和告警的展示,安全管理员可根据业务节点的重要性按照不同优先级处理业务节点的安全风险。

当发现某个流程节点的风险之后,能够在流程节点上进行处理操作,包括关联知识库信息、立刻进行告警派单处理、对于不必要派单的告警信息可支持手动清除等。通过及时把告警风险派单到该业务系统或资产的负责人,有效地消除风险。

4 基于业务流程粒度风险管理应用效果

通过 BSMP 的部署和推广实施,把 WAP 系统和短信系统纳入业务流程风险管理范围,短信业务流程监控管理界面如图 4 所示。

- WAP 系统的业务流程划分为 MS、GGSN、WAP 网关、DNS、SP 应用服务器 5 个业务流程节点。

- 短信系统的业务流程划分为 SMC、HLR、MSC、VLR、BSC&RNC、MS 6 个业务流程节点。

通过短信业务流程监控管理,可监控每个业务流程节点的风险状态,并在每个业务流程节点上关联查看和处理相关节点的资产对象安全告警。

通过基于业务流程粒度的风险管理,安全管理员和业务系统管理员可清晰了解业务系统各个流程环节的安全风险状况,有效聚焦和优先处理业务系统关键业务流程的安全告警和风险;安全主管可基于业务流程感知安全风险态势,并有针对性地规划、制定和实施安全防护方案。

随着基于业务流程风险管理的推广应用,有效定位业务流程环节的安全风险,并根据业务流程环节的重要性和风险状态,自动生成安全风险告警处理的优先级顺序,真正实现基于业务的安全防护。

5 结束语

本文分析了现有安全风险模型的不足,并结合电信运营商的业务特点,设计了基于业务流程粒度的安全风险模型。依托业务流程风险管理,将设备安全提升至业务安全层面,实现了通过业务流程粒度分析和展示风险,满足企业对业务安全风险管理的需要,提高了信息安全管理水平。

参考文献

- 1 李斌,王声远,鲍旭华等. 基于业务流程状态分析的风险评估. 清华大学学报(自然科学版), 2009(S2)
- 2 温乃粘. 加强流程风险分析,防范业务流程风险. AMT 前沿论丛, 2011(3)

(收稿日期:2013-10-20)