



业务平台安全解决方案研究

王艳春¹, 李洪²

(1. 中国电信股份有限公司宁夏分公司 银川 750001;

2. 中国电信集团公司网络运行维护事业部 北京 100032)

摘要:电信业务平台作为重要的支撑系统,需确保业务系统及各类信息数据的安全,尽量避免安全事件带来的负面影响及经济损失。从实际出发,通过调研及问题溯源分析,阐述电信业务平台安全方面的几个典型问题,以流程为切入点,结合管理和技术两个维度,探讨研究业务平台安全问题的解决方案。

关键词:业务平台安全;流程管理;接入层面安全;终端安全管理

doi: 10.3969/j.issn.1000-0801.2013.08.014

Research on the Solution of Business Platform Security

Wang Yanchun¹, Li Hong²

(1. Ningxia Branch of China Telecom Co., Ltd., Yinchuan 750001, China;

2. Network Operation & Maintenance Division, China Telecom Corporation, Beijing 100032, China)

Abstract: As an important support system, it is necessary for the telecommunication service platform to ensure the security of service system and the information data, and to try to avoid the negative effects brought by security events and economic loss. Based on the research and analysis, several typical problems of safety telecommunications business platform, and the entry point for the process, were studied. At last, with two aspects of management and technology, the solution to security problems of service platform was discussed.

Key words: business platform security, process management, access layer security, terminal security management

1 前言

电信业务平台作为增值业务的重要支撑系统,密切关系公司运营,直接影响用户感知。在保障公司规模发展的大前提下,如何保障可持续性发展,确保业务系统及各类数据信息的稳定、安全,尽量避免安全事件带来的负面影响及经济损失,提升业务平台安全防护,已经成为电信业务运营中不可忽视的重要环节。

较典型的电信业务网在全国具备统一的架构,体现“统一管理、统一鉴权、统一计费、统一门户、统一接入”的特点,各省的业务平台存在很大的共性。笔者选取几类业务平台共性的安全问题,从管理和技术相结合的角度,探

讨研究业务平台安全问题的解决思路。

2 业务平台安全问题

业务平台对电信公司规模发展的贡献越来越突出,平台种类及相互间的关联也越来越多,逐渐出现了一些因恶意攻击、信息泄露或业务套用、盗用的恶性安全事件,给业务运营商造成很大的经济损失,降低了用户对运营商的信任度与忠诚度。从实际出发,从业务运营中发现一切可能存在的漏洞及隐患类安全问题,积极制定解决方案并提前预防,成为支撑移动业务运营的又一项新的挑战。

结合全网通用业务平台,笔者调研了 ISMP、ISAG、WAP GW、MMSC、彩铃、消息综合平台等业务平台,采用流



程梳理和漏洞扫描的方式,归纳、分析整体业务平台安全方面存在的问题,主要层面及处置难度介绍如下。

- 应用层面:业务逻辑、业务鉴权、Web 应用等存在漏洞,涉及版本开发需求、多个应用系统、不同厂商,存在兼容性问题,操作风险大,需资金投入。
- 功能审计:设备自身日志难以展现安全事件,安全审计功能薄弱,不能实时预警,人工审计耗费人力,实时性不高、效率不高,涉及版本开发或新系统建设,需资金投入。
- 主机层面:服务器操作系统、数据库、应用系统中间件等存在不同程度的安全漏洞,需实施补丁投入,但因涉及与应用的关联,存在兼容性风险,且需资金投入。
- 网络层面:访问控制策略缺失或较粗放,安全域的划分不合理,需对现网已商用平台重新进行规划、调整,操作风险较大,需资金投入。
- 业务数据:用户数据、用户属性、用户行为记录等敏感信息,有些以明文方式呈现、传送,涉及版本开发、接口规则变更及调测,需资金投入。
- 接入层面:平台周边业务接口种类繁多,信息交互规则有待规范,终端使用者不唯一,外围接入终端使用形式较多,稍有疏漏便存在信息泄露的风险,需规范、细化接入标准,提升管理手段,需资金投入。

对以上问题的出现原因追根溯源,所涉及的因素有些为单一因素,有些则是多种因素共同导致,介绍如下。

2.1 业务平台先天缺陷问题

业务平台在特定的需求环境下,陆续投入电信业务运营行列,平台厂商众多,开发水平参差不齐。为适应业务多样性及开放的时效性,业务平台厂商往往为推出特色业务,将重心放在业务功能实现上,在业务平台是否具备运营条件所需的各安全要素上缺乏模块的支撑。例如,很多平台维护管理能力薄弱,缺乏对维护界面告警监控、统计分析、重要网元的维护操作,缺乏权限管理策略,缺乏安全审计类功能;有些平台业务逻辑或核心流程存在漏洞、隐患,易被非法套用、盗用。另外,平台厂商所选硬件,尤其是软件与应用存在一定的对应绑定关系,其适用的操作系统、数据库版本以及 Web 应用等,可能存在较大的安全漏洞,但因涉及与应用的兼容性,不能随意变更或升级。这些问题均来自平台自身,一旦进入电信业务运营支撑网络,

就会因携带先天缺陷而带来安全问题。

2.2 业务入网规划及后期改造规划的管理

因电信业务的个性化要求较高,业务实现流程复杂,尤其具备漫游属性的业务,整个业务运营涉及集团级、各省级多类网元,运营商对业务需求的确立、业务入网的把关及网内业务部署方案的规划,是最重要的管理阶段。规划设计方案指引平台建设各环节,确定组网结构、实施方案、业务功能联调以及维护支撑模块框架。如果运营商在入网规划或后期改造规划中出现疏漏,就会导致业务安全问题。例如,有的平台内组网结构混乱、网络出口无访问控制策略、平台网络未划分域或域的划分不合理;有的综合管理类平台和综合网管类平台,实现方式和组网规划不严谨,在接入整个业务网络后成为短板,降低整个业务网的安全防护水平;有的平台规划中核心设备出现单节点,重要的上联节点未考虑容灾性,没有防病毒机制;有的平台业务需求设计存在缺陷,鉴权流程太弱或业务实现中需由其他平台开放核心业务数据作为数据源,自身安全管理存在漏洞也给其他关联业务带来很大的安全隐患。

2.3 建设、维护、运营流程的安全管理

业务平台因个性化,实现模式基本不重复,在建设及开放初期往往需要摸索探路,为抢占市场先机,很多是在时间紧、任务重以及相关规范还在逐步建立的情况下建成投产,运营后需付出很多人力、物力和财力进行安全加固和整治。在工程建设及改造项目实施中,因实施不规范或操作管理薄弱,会出现安全问题,如开局中账号、口令不符合安全策略,有些账号内置到应用后不能随意修改,后期改造十分困难;部分平台开放了很多不必要的端口、服务,存在防火墙策略过于粗放、安全配置不合理等问题。有些平台上线后,为了支撑一些特殊业务需求,提供专项接入,而第三方接入设备的安全措施、维护能力难以管控,存在安全隐患。

平台入网后,建设之前、之后各个环节遗留的问题以及伴随网络变更、业务调整、设备老化、技术更新等过程带来的新问题,都会给运维支撑工作带来很大的负担,这个时期成为安全风险的高发阶段,因此必须对整个业务运营工作的流程管理提出更高的要求。

2.4 业务运营数据的安全问题

业务运营支撑中,要做好安全保护的运营数据包括用户类信息和公司运营数据,其中,用户信息数据包含用户个人账号口令、个人资料、业务属性信息及用户行为轨迹

信息,公司业务运营数据包含平台业务统计数据、平台管理账号口令、网络结构拓扑及配置信息。这些数据在不同的平台中有不同的管理方式,很多平台缺乏密级设置和加密策略,在数据存储、查询或数据流传递过程中缺乏有效的保障机制,存在安全隐患,如果发生泄露会给公司带来不同程度的经济损失和负面影响。

2.5 人员及接入终端安全问题

分析目前已经出现过的业务平台安全事件,人为原因造成管理疏忽、数据配置变更、信息泄露、恶意破坏、恶意入侵等行为所占的比例相当大。在业务系统的整个生产运营中,涉及各类人员数量众多,掌握重要信息、能进入核心系统的人员不在少数,人员的素质和水平与业务平台的安全稳定息息相关。另外,当前业务系统通过层层网络安全部署,一般外部人员很难对核心系统造成威胁,有机会接触企业业务的内部人员或者第三方维护人员则可能成为一个薄弱点,突破口最大的可能就是接入终端。在接入层面很多终端都缺少安全管控,对软件的安装使用、账号密码设置、行为审计都无法监管,有些专用终端还多人共用、跨接外部网络。这些问题可能会导致信息泄露、恶意软件传播等破坏行为,而事后追究十分困难。为了避免公司内部人员或者第三方维护人员,有意或无意造成信息泄露或行为破坏,必须要重视对人员及终端的安全管理。

3 管理与技术结合,探讨解决方案

电信业务从需求的提出,到规划、建设、运营和维护支撑,由多个环节或部门经手负责,环环相扣,每个环节产出结果是否达标,安全责任是否执行到位,决定了下游环节工作开展所处的高度,业务安全的意识必须贯穿始终。解决业务平台安全问题,要本着“预防为主,整治为辅”的思路实施“两步走”策略,一个是以防为主,从流程入手环环相扣,提倡精细化管理,优化相关工作流程;另一个是以治为主,聚焦业务平台一系列安全问题中的关键性问题,利用技术手段整治解决。通过上下联动的方式,激活电信公司集体活力,整改见效后可以有效整合各项支出与投入比例,节约专项支出转变为隐形效益,助力公司集约运营、规模发展,同时集中优势资源,支撑重点业务的运营。

3.1 优化产品规划开发,严把设备入网关

平台厂商做业务产品的设计开发主要来源于两种需求:一个是运营商的需求定制,一个是厂商自主研发。以往的业务平台产品在需求规划阶段缺乏专项的安全审查,后

期产品定格或上线后发现问题,再进行改造、修补工作,既耗费时间、人力和物力,又影响业务提供的稳定性和用户感知,后期改造的效果也难以管控。为了解决产品层面的安全问题,要求运营商和厂商在业务产品需求的规划期就开始入手,增加安全评估环节,必须对产品附加安全约束。

解决办法是在业务需求评估前,制定一套满足移动业务运营类需求的安全评估模型,将总体功能模块化,做好横向和纵向审查。横向审查要求产品具备以下基本要素:业务接入管理功能、网元管理功能、告警监控功能、统计分析功能、业务数据管理功能、账号分权分域管理功能、安全日志管理审计、数据配置管理等功能,各要素间的关联分界要清晰,数据吞吐规则要明确,评估系统的物理布局、组网架构是否合理,是否部署安全保护措施等;纵向审查要求深入各功能模块,至少评估各软件及应用版本是否达标、渗透分析业务逻辑及嵌套关系,评估内部数据安全存储、访问策略,评估对外接口协议及边界保护措施等。

通过这种安全评估审查,可进一步完善业务需求规划,在产品开发中增加安全部署,在产品入网前做好安全审查,势必可以减轻后期施工建设、维护及安全整治中的大量工作。

3.2 建立健全产品和服务的认证机制

业务平台内部的安全问题涉及产品和服务问题,产品问题主要在平台新建、扩建阶段,涉及硬件厂商、软件及应用提供厂商、系统集成商;服务问题主要在后期维护支撑阶段,涉及维保厂商和安全厂商。各厂商与电信业务的生存及质量保障关联密切,为了解决业务平台层面存在的安全问题,要供给双方均付出努力,把握好制约与协作,建立双方共赢的合作关系。

购置业务平台产品和购买维修、维护服务,涉及与多类厂商的协作,厂商的内部管理和人员的技术水平参差不齐,服务质量会直接影响业务平台产品质量。为了提高厂商对产品和服务的安全意识贯彻效果,需要适度地引入竞争机制。解决办法是建立健全一种移动业务产品和服务的认证机制,为关联厂商建立合作档案,跟踪合作事宜、产品质量、性价比、安全事件、处理反馈效果等内容,通过形成有效的评估机制,对关联厂商进行资质分级,分出优良中差,做得好的晋级奖励,做得差的根据评估规则降级处分。建议至少半年做一次,对于连续评优的厂商赋予一定优先权,在出现同类产品竞争中,可享有一定的加分。

建立健全这种机制,可以树立厂商良性竞争势头,通



过优胜劣汰,加强企业自主安全意识,在开发生产过程中,尽量加大对安全防范的规划、选择及投入力度。

3.3 优化流程、精确管理,以防为主提升运营安全管理效率

公司整个的业务运营管理工作从业务需求规划、方案部署、建设实施,到上线商用的业务运营、维护支撑、信息管理分析,涉及很多工作流程和部门职责。工作流程是不同时期顺应业务运营而形成的,伴随网络不断的发展,目前的业务网包含了固网、小灵通网、CDMA 网以及近年新建的 IMS 网,业务种类及关联关系众多,业务流程各异,工作流程很繁杂。中国电信集团公司和省分公司陆续下发了各类安全管理办法、职责划分、行为规范、操作指引、安全验收等文件,逐步规范和明确业务安全管理工作的要求,省内要结合实际加以贯彻、落实,注重实效。

从流程管理角度分析还存有优化的空间,可以通过优化流程,加强精确化管理,解决并预防因工作流不畅、上下衔接监管不力或责任范围变更不清晰等因素综合导致的业务安全问题,将最好的人力、物力有效地运用于核心工作流程,提高管理工作效率。

优化流程要随着业务周期的变化持续调整,通过对工作重心做出一定的调整,适时简化掉一些历史留存的无增益的工作流,优化人员配备。目前主要平台已经进行了等级区分,维护级别要求不同,但因现网的业务变更频繁,关联关系错综复杂,各平台的维护能力、防护能力存在较大差别,难免会出现“短板效应”,某个疏忽漏洞就可能对整个业务网络形成安全威胁。为了优化流程,加强防护能力,一方面要尽快梳理出那些非标准化高风险平台和老旧的低效益平台,加紧转网或退网,消除隐患、简化流程、减轻维护负担;另一方面要根据公司发展战略适时转移重心。新业务筹备实施前,要提前确定好业务管理、业务监管相关的配套流程,保障业务平台一开始建设就有统一的管理氛围,降低厂商产品先天缺陷牵制业务运营的风险,杜绝目前存在的某些业务平台建成后,缺乏针对性业务运营规范,不明确业务管理负责人的被动运营局面。第三方面要推进建立标准化维护管理模式。目前的维护模式受责任划分、考核机制等因素,很多平台的维护还是责任人包局模式,事务繁杂且专业综合性很强,专业化维护程度很难深入,平台维护能力和包局数量受个人素质、技术能力制约,维护人员职业发展困顿。要解决需着力研究维护工作管理模式,将整个维护工作进行有机的切割,做好分段技术管理和统一融合管理,建立一种标准化维护管理模式,夯实

基础维护工作,整体提升基础维护能力。最后要加强 SOC 体系建设。通过专业化手段,提升业务平台安全防护工作的层次和深度,通过持续推进 SOC 平台安全子系统建设,发挥 SOC 平台的安全事件管理、安全风险分析等作用,推进集中化全网安全监控管理能力。

流程优化中也要提升精确化的管理效率,需要一套综合性较高的运营支撑系统,以产品的生命周期为主线,将运营中的各环节纳入其中,实现统一管控,辅助调整工作侧重点,提高效率。当前各个电子管理系统基本上是分管一片,不能实现全业务运营流程的管控,短期内很难构建出一套完善的综合管理系统,因此要借助人员管理上的努力,衔接起各系统间的流转,为此公司要针对几个薄弱点增加监管环节,加强部门间合作与监督,每个部门将安全责任切实纳入日常工作管理流程,才能减轻下一环节的负担。

3.4 有的放矢,实施专项技术整治

业务运营中的安全问题,不可能通过预防的方式全部杜绝,随着网络变更、技术更新,有些关键性问题必须借助技术手段进行专项整治。

在业务平台网络层面安全问题中,亟待解决的是有些平台内部组网过复杂、内部子网间以及外部访问控制不严格等问题,重点业务受到安全威胁。解决方案复杂、周期较长、操作风险大、对业务影响时间长。解决这一问题要借助技术手段,依据承载业务的分类和安全防护级别对系统做层次划分,以便分别制定安全保护措施。采用的方法是基于对业务平台网络和业务的充分理解,在保证业务正常开展的同时,采用安全域划分和边界整合的方法进行专项整治。

安全域是指同一系统内有相同的安全保护需求,相互信任,并具有相同的安全访问控制和边界控制策略的 IT 要素集合,相同的安全域共享相同的安全策略。安全域划分的主要原则,是要保障业务正常运行,不能改变原有责任界面和维护界面,通过分析系统风险、安全需求,在一定程度上分解、简化系统结构,对属于同一安全域内的系统应互相信任,建立评估与监控机制,设计防护机制的强度和保护等级。边界整合是在安全域划分的基础上,对保护等级、功能、通信方法相同或相似的区域进行整合,对系统与网络接口进行有效的整理和归并,减少接口数量,提高系统与网络接口的规范性,实现对安全域进行安全防护。

通过使用安全域划分和边界整合方法实施业务平台专项整治,可使业务平台形成清晰、简洁的网络及组网架

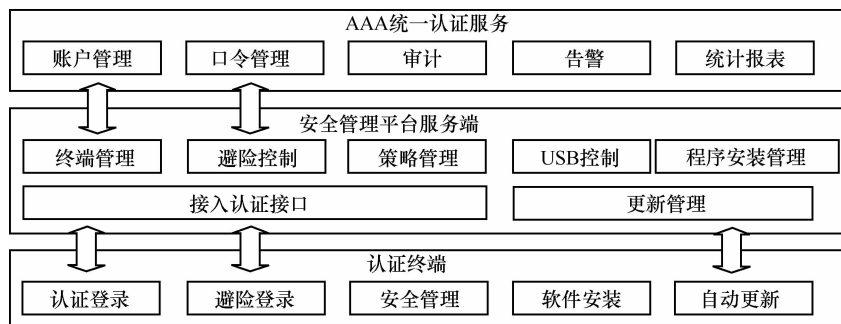


图 1 宁夏电信终端安全管理系统架构

构,实现相关网络与系统之间严格访问控制的安全互连,才能更好地解决复杂系统的安全问题,提升业务平台安全整治的成效。

3.5 拓展人员安全意识,解决接入层安全管理问题

人员管理是将安全管理深入最小单元,要提高人员业务能力、技术水平,也要提高人员的安全意识和忠诚度,提高综合素质,形成行为约束才能降低人为原因造成的安全事件。人员管理涉及内部人员和外部人员,首先要制定人员安全方面的管理办法,明确内、外部人员的访问操作管理措施和审批流程,明确每人的工作角色和工作职责。其次,对涉及核心系统、高安全级别的内部人员和第三方人员签署保密协议,制定安全考核措施。另外,企业要通过一系列定向的培训、宣贯、实践锻炼,既增加员工技能培训,也要在全员范围内深入拓展安全意识培训,给员工积极向上的动力,引导员工职业发展规划,培养各级人员忠诚度,树立人人将安全防范贯彻到底的决心,只有每个人守好一方阵地,整个企业才有凝聚力、竞争力,安全才有保障。

在强化人员管理的同时要重视接入层安全管理,操作终端作为最普通、最常用的接入层面实体设备,通过它可以进入业务系统内部,获取到命令操作和数据访问的权限,电信业务运营支撑中每日都离不开它,做好接入层面的安全管理,具有很重要的现实意义。此外,接入终端的使用首先需经过授权许可,在这个点上通过技术手段,做到入口把关,并注入相关安全策略加以管控,是有可操作性的。

问题解决的核心思路是从接入、认证、鉴权、审计方面,对接入终端进行统一管理,通过在管理服务器制定详细的安全策略,与接入客户端实现控制信息交互,保障对接入终端的管控能力。这个解决方案目前在宁夏电信做试点,宁夏电信终端安全管理系统的系统架构如图 1 所示。

方案主要设计部署一套终端安全管理系统,包括统一

认证服务模块、客户端模块和服务端模块 3 部分。直观上通过手机动态密码的方式,实现终端管理账号与申请操作人员的有效映射关系,对每次有效的系统登录进行实时的短信验证授权,同时进行登录、登出审计管理,此外,通过部署下发的安全策略负责对系统安全进行监测、控制、处理和审计。

目前通过一期试点,可以管控操作人员与终端使用的对应关系,有效防止未经授权的系统登录及访问等操作。另外,可记录登录、登出及相关审计日志,做到防恶意登录卸载、避险登录,在约束人员操作行为和管控接入终端的使用上收到成效,在解决业务平台接入层面安全管理问题上值得借鉴。

4 结束语

移动增值业务在给人们带来诸多便利的同时,平台安全、网络安全、信息安全问题日益突出,伴随各类互联网技术不断发展,各类业务应用的关联越发错综复杂,各种各样的攻击手段也层出不穷,安全的威胁在不断扩散。业务平台安全防护工作是一项长期的工作,不可一蹴而就,需不懈地探索、钻研,通过不断发现问题并从中提炼关键性问题,借助电信运营商的管理经验,针对性结合行业内管理理论、技术手段,各个击破,提升安全防护水平,创造隐形效益。

参考文献

- 1 中国电信集团运维指挥[2010]1261 号. 中国电信增值业务平台安全管理办法(试行), 2010
- 2 中国电信集团运维指挥[2011]. 中国电信互联网及相关网络安全域划分与边界整合技术规范, 2011
- 3 中国电信集团运维指挥[2011]1701 号. 中国电信业务平台等级安全基线规范(试行), 2011

(收稿日期:2013-08-01)