|  |  |
| --- | --- |
| 产品名称 | 密级 |
|  | 机密 |
| 产品版本 | 共20页 |
|  |

营销管理系统安全性威胁分析及需求说明书

Marketing Management System Security Threats Analysis and Requirement Specification *(Title must be in both Chinese and English to facilitate English speaking users' search为方便英语用户检索，此处必须提供中英文版)*

|  |  |  |  |
| --- | --- | --- | --- |
| 拟制 | 史习云 | 日期 | 2015-12-01 |
| 审核 |  | 日期 |  |
| 批准 |  | 日期 |  |



华为技术有限公司

版权所有 侵权必究

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 修改描述 | 作者 |
| 2015-12-01 | 1.0 | 初稿完成 | 史习云（00359263） |
| yyyy-mm-dd | 1.1 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目 录

[1 系统概述 6](#_Toc408235297)

[1.1 系统描述 6](#_Toc408235298)

[1.2 产品组网 6](#_Toc408235299)

[2 目标市场安全需求分析 6](#_Toc408235300)

[3 High Level威胁分析 6](#_Toc408235301)

[4 安全基线（含红线）需求分析 6](#_Toc408235302)

[5 竞争力安全需求分析 6](#_Toc408235303)

[6 其他安全需求分析 6](#_Toc408235304)

[7 安全需求汇总 6](#_Toc408235305)

[8 备注和附录 7](#_Toc408235306)

表目录

图目录

Keywords 关键词： *Provide Keywords in both Chinese and English to facilitate English speaking users' search. 为方便英语用户检索，此处必须提供中英文版*

Abstract 摘要：*Provide Abstract in both Chinese and English to facilitate English speaking users' search. 为方便英语用户检索，此处必须提供中英文版*

术语和缩略语清单：

| 术语/缩略语 | 描述 |
| --- | --- |
| MPLS (Multiprotocol Label Switching) | MPLS（多协议标签交换）是提高电信网络性能的一种机制。在MPLS网络中根据数据的标签确定下一跳的节点 |
|  |  |
|  |  |
|  |  |

# 系统概述

## 系统描述

本章节简要描述待开发系统的运行及部署环境，描述产品主要实现的业务功能。

华为智能终端越来越火爆，线上线下越来越抢手。为了支撑日常的终端的营销，我司需要在各个门户投放广告。选择哪些门户、哪些广告位进行广告的投放，广告投放的效果如何，我们需要设计这么一套系统，在跟踪分析终端广告投放的效果。

1、创建营销活动，每个活动产生多个广告位。对于每个广告位的着陆链接进行生成监控代码，后续广告投放时，就会通过http消息上报对于的数据。

2、将数据平台获得的数据进行统计，将统计出来的汇总值在系统中展示。

## 产品组网

本章描述产品的组网环境及组网图，对于组网环境不确定的情况，描述出典型业务场景组网。对于终端没有组网的产品，这里建议使用的业务场景架构图。



# 目标市场安全需求分析

*针对产品的目标市场及客户，分析目标市场是否有明确的安全性需求，或客户是否有明确的安全需求，本章描述这些显示化的安全需求。*

系统为华为公司内部使用系统，无市场安全需求。

# High Level威胁分析

## 1-DFD

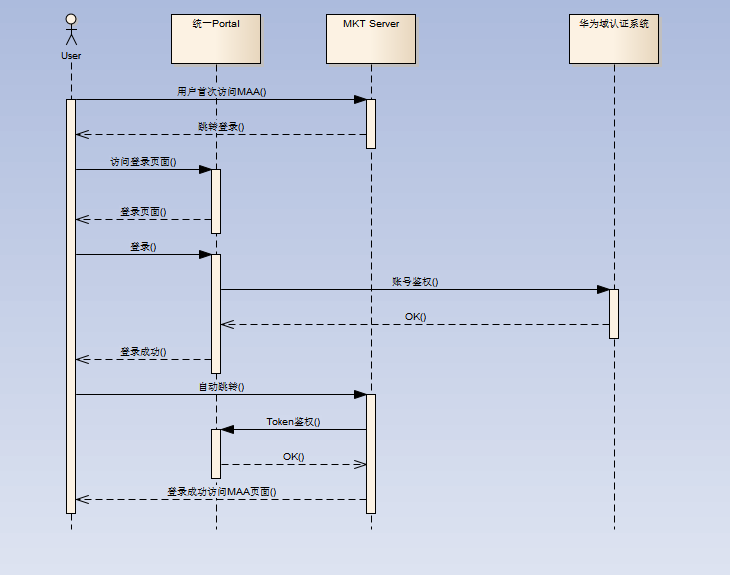
### 数据流图



### 业务场景及信任边界说明

涉及信任边界的业务场景主要包括数据统计、用户登录（查看报表）、发送邮件活动三个场景

#### 用户登录



信任边界主要为网络边界：

用户与MKT Server、MKT Server与统一portal 、MKT Server和邮件服务器为网络边界，信任度较低。

注：统一Portal华为域认证服务器之间为IT机房内部网络信任度较高，且MKT Server不直接与域认证服务器交互，此处不做分析。MKT Server和邮件服务器亦然。

#### 数据统计

MKT Server：用户在MKT中配置应用信息存储在MySQL中，用户的所有的日志操作也存储于Mysql中

Hadoop(BI数据仓库)：负责根据上报数据信息离线统计各类应用数据，统计完后数据同步到MySQL，以供前台展示使用。

该场景中，MKT Server、Hadoop部署在统一网络内，之间使用内部IP进行通信；信任度较高可以作为内部威胁来分析。

### 攻击面分析及最小化



### 外部交互方分析

#### Hadoop

|  |  |  |
| --- | --- | --- |
| 元素名称 | Hadoop | |
| 元素概述 | 支撑后台数据 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 统一Portal

|  |  |  |
| --- | --- | --- |
| 元素名称 | 统一Portal | |
| 元素概述 | 包括统一Portal和华为IT机房域认证系统 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **不分析：在信任边界内**  内部信任系统 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **不分析：在信任边界内**  内部信任系统 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 用户

|  |  |  |
| --- | --- | --- |
| 元素名称 | 用户 | |
| 元素概述 | NA | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  用户被仿冒,可以配置查看系统的数据  【可能性】  1. 同时获得vpn账号、vpn证书和华为员工域账号密码  2.同时获得iaccess接入权限和华为员工域账号密码  **可能性评估：**  无 |
| 已有消减措施 | 1.使用公司域账号进行认证  2.必须接入iaccess或vpn才能访问  3.使用https通道 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  修改系统配置信息  【可能性】  获取授权系统账号及数据库账号删除操作日志数据  **可能性评估：**  无 |
| 已有消减措施 | 1.只有运维人员通过vpn才能访问业务数据库  2.只有授权的Linux账号才能访问数据库并删除数据  3.通过接口等方式也无法访问日志数据  4.根据运维管理制度，运维人员定期修改密码 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |

#### 邮件服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 邮件服务器 | |
| 元素概述 | NA | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

### 数据流分析

#### Hadoop⇒MKT Server(数据导出)

|  |  |  |
| --- | --- | --- |
| 元素名称 | Hadoop⇒ MKT Server(数据导出) | |
| 元素概述 | NA | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### MKT Server⇒邮件服务器(发送邮件)

|  |  |  |
| --- | --- | --- |
| 元素名称 | MKT Server⇒邮件服务器(发送邮件) | |
| 元素概述 | NA | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 统一Portal⇔MKT Server(认证Token/用户信息)

|  |  |  |
| --- | --- | --- |
| 元素名称 | 统一Portal⇔MKT Server(认证Token/用户信息) | |
| 元素概述 | MKT到统一Portal认证token是否合法,统一Portal同步用户信息到MKT | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  影响业务登录,同步错误的用户信息  【可能性】  网元被劫持篡改数据  **可能性评估：**  无 |
| 已有消减措施 | 1.https传输，认证证书  2.认证消息头和时间戳 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  泄露用户token信息  【可能性】  网络嗅探抓包分析  **可能性评估：**  无 |
| 已有消减措施 | 1.https传输 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  攻击者发起大量请求导致统一Portal拒绝服务  【可能性】  攻击者模拟消息请求  **可能性评估：**  无 |
| 已有消减措施 | 1. 访问设置白名单IP控制  2.https配置证书认证  3.前段设有防火墙及Nginx进行流控 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |

#### 用户⇔MKT Server(操作请求/Token/响应结果)

|  |  |  |
| --- | --- | --- |
| 元素名称 | 用户⇒ MKT Server(操作请求/Token/响应结果) | |
| 元素概述 | 用户配置应用信息，查询统计数据 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  数据被篡改后MKT执行错误的操作，用户看到异常的结果  【可能性】  劫持网元修改数据流内容  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.https加密传输 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | 1. 无 |
| 信息泄漏（I） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  泄露用户token及数据统计结果  【可能性】  网络抓包分析  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.https加密传输 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | 1. 无 |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  恶意攻击导致MKT拒绝服务  【可能性】  模拟数据攻击  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.域账号密码认证  3.设置有防火墙进行流控 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | 1. 无 |

### 处理过程分析

#### MKT Server

|  |  |  |
| --- | --- | --- |
| 元素名称 | MKT Server | |
| 元素概述 | 为用户提供操作入口,配置应用信息、查询统计数据 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  仿冒MKT为客户端浏览器提供服务  【可能性】  用户本地hosts被修改，或者DNS被劫持，导致用户 访问到仿冒的钓鱼网站  **可能性评估：**  无 |
| 已有消减措施 | 用户本地需要是vpn或iaccess接入，规避DNS被篡改 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |
| 篡改（T） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  影响正常的业务逻辑  【可能性】  利用输入通道注入，获取相应权限篡改程序  **可能性评估：**  无 |
| 已有消减措施 | 1. 代码层面完成安全编码（codecc、代码检视等）  2.系统层面通过appscan扫描 防止出现注入  3.系统运行环境和容器定时更新漏洞 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  修改系统配置信息  【可能性】  获取授权系统账号及数据库账号删除操作日志数据  **可能性评估：**  无 |
| 已有消减措施 | 1.只有运维人员通过vpn才能访问业务数据库  2.只有授权的Linux账号才能访问数据库并删除数据  3.通过接口等方式也无法访问日志数据  4.根据运维管理制度，运维人员定期修改密码 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  影响】  泄露系统信息  【可能性】  1.利用漏洞获取特权  **可能性评估：**  无 |
| 已有消减措施 | 1.系统中不存在涉及用户隐私的数据  2.appscan扫描防止漏洞出现  3.codecc 检查、规范日志 防止泄露系统信息  4.系统运行环境仅运维人员通过vpn接入才能访问 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  系统提供服务相应变慢  【可能性】  恶意用户Dos攻击  **可能性评估：**  无 |
| 已有消减措施 | 1. 内部系统，必须通过iaccess/vpn访问，用户量较少，且有操作日志。可以减少恶意攻击的风险  2. 关键资源有排队机制，超出范围数据等待  3.提供主备倒换能力  4.系统设有防火墙减少恶意攻击  5.运维对cpu、内存等使用情况有监控机制 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |
| 特权提升（E） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  获得高级权限，查看高级数据或执行高级操作  【可能性】  低  **可能性评估：**  无 |
| 已有消减措施 | 1.账号使用华为域账号  2.权限基于角色进行管理  3.使用拦截器实现用户权限控制  4.以单独的linux账号运行程序，且仅分配必须的权限 |
| 建议消减措施 | 1. 无 |
| 产品落地计划 | NA |

### 数据存储分析

# 安全基线（含红线）需求分析

*本章描述除了目标市场与威胁分析之外的，又属于基线（红线）要求的内容的需求*

*例如：支持限制同一用户的在线数目*

*1、基于安全可审计原则，一个自然人只对应一个唯一的操作维护用户，因此系统应支持限制同一用户同时多处登录，即限制同一用户的最大在线数目。*

*2、对应网元来说，在实际应用中存在不同的维护工具，因此同一用户在同一终端上可能同时使用多个工具，因此系统应支持允许同一用户多实例登录。*

*3、基于以上考虑，网元应支持同一用户的最大在线数目可管理，由管理员根据需要设置允许同一用户同时从不同客户端登录的数目。*

*4、系统应默认只允许一个用户在一处登录。*

**

# 竞争力安全需求分析

*本章描述通过对友商产品进行安全性分析，提炼构建产品在安全领域的竞争力方面的需求，如没有竞争力相关的需求，本章可省略*

# 其他安全需求分析

*描述除了上述分类之外，其他的安全需求*

**

# 安全需求汇总

*如果需求较多，可以在此处嵌入Excel表格作为附件，格式要求与下表相同*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *序号* | *需求描述(引用威胁分析中所有建议的消减措施)* | *优先级(高、中、低)* | *落地计划* | *需求来源* |
| 1 | 权限控制，对于用户必须有严格细致的数据权限控制，可以控制到应用、产品粒度 | 高 | 当前版本 |  |
| 2 | 广告位录入优化 | 高 | 当前版本 |  |
| 3 | 流量报表优化 | 高 | 当前版本 |  |
| 4 | 新增转化报表报表 | 高 | 当前版本 |  |
| 5 | 支持导流到第三方平台的广告监控 | 高 | 当前版本 |  |
| 6 | 日志查询 | 中 | 当前版本 |  |

# 备注和附录

本章节描述需要说明的附加内容。

参考资料清单：

请罗列本文档所参考的有关参考文献和相关文档，格式如下：

作者＋书名（或杂志、文献、文档）＋出版社（或期号、卷号、公司文档编号）＋出版日期+起止页码

例如：

1. D. B. Leeson, “A Simple Model of Feedback Oscillator Noise Spectrum,” Proc. IEEE, pp329-330, February 1966
2. D. Wolaver, Phase-Locked Loop Circuit Design, Prentice Hall, New Jersey,1991