宁波市轨道交通集团有限公司运营分公司

办公网络安全监测系统采购项目

(办公网络安全评估系统采购项目)

需求部门：企划部

2016年 8月 5 日

1. **项目背景**

宁波轨道交通1号线一期、2号线一期及1号线二期已经投入运营，随着信息终端数量不断增加、专业管理软件系统建设不断地发展以及轨道交通各区域的办公网络不断地完善，不同区域的系统安全管理工作难以集中监管、防范风险。信息安全威胁的形式也趋于复杂，攻击方式从个人攻击，向有组织、有规模的攻击转变，用户也可能因无意识的情况下下载某些软件或开放某些不必要的端口和服务从而成为某些网络攻击的对象或跳板，使系统风险成倍的增加。

1. **项目必要性**

**2.1**随着1号线二期开通，目前运营公司办公网络中共有二百五十余台网络交换机，八百余台办公电脑分布在OCC大楼、2个车辆段、3个停车场、1号线29个车站、2号线22个车站，分布很广，很难监控办公网络中设备安装的操作系统、软件是否不符合要求，是否在办公网络中私自架设服务器、共享文件夹是否存在风险以及其他违反办公网络管理办法的行为，本系统可以集中管理和监控办公网络上所有的信息化设备。集团目前的上网行为记录仅针对互联网的上网行为进行监控，没有针对内网的相关行为监控和管理。

**2.2**因信息化建设速度加快，重要信息系统数量增加，系统复杂程度提高，业务依赖信息化程度增强，信息技术已日益成为运营分公司提高管理水平、服务质量和工作效率的有力手段。运营分公司为贯彻落实国家信息安全相关要求以及满足自身信息系统安全管理的需要，积极开展信息安全防护、测试、检查等工作，提高信息安全保护与信息安全技术水平，建立保障重要信息系统安全稳定运行的长效机制，对促进轨道交通信息化建设，增强安全防范能力，提高运行保障水平，确保信息系统安全稳定运行具有重要意义。

**2.2**目前办公网络管理员和信息系统管理员缺少相应的管理和分析工具，对网络上和系统上的异常行为只能进行被动的调整和修复，不能做到及时有效的定位相关设备和设备的具体异常行为和风险，本系统可以预先对异常行为和风险进行评定和分析，提出具体的解决方案。

**2.3** 根据《信息系统安全管理办法》要求，拟引进第三方咨询检测公司对运营公司范围内的办公网络系统和运行在办公网络上的信息系统出具风险监测报告。

**2.4**信息安全作为信息化的日常工作之一，需要根据最新的形势对信息化安全工作小组各个成员进行相关的信息安全培训，而我们目前缺少最新的信息安全培训的资料（包括PPT课件、视频以及相关纸质文档）这个项目可以有效的提高信息安全培训的质量。

**2.5**对信息安全管理人员的素质提高也是做好信息安全工作的重要一部分，本项目可以对信息系统安全管理人员进行培训和相关认证，确保其能及时掌握最新信息系统安全管理方法及相关技术和检查手段。

1. **项目总体目标和实施范围**

**3.1** **项目总体目标**

通过该项目的实施，达到扫描及监控办公网络和运行在办公网络上的信息系统安全、发现漏洞、弱口令、各类不必要开启的端口和服务，监测企划部机房，定期提供风险报告以及必要的信息安全培训，从而达到建立健全运营分公司层面的信息系统安全工作规范、有效地提高信息系统安全管理水平，从而为运营分公司供良好的信息系统安全保障。

**3.2 主要实施内容及范围**

3.2.1实施内容

* 办公网络安全监测系统建设
* 信息系统安全业务咨询服务
* 相关信息系统安全培训

3.2.2 实施范围

1号线一期、2号线一期、1号线二期（包括但不限于车辆段、停车场、车站等运营场所）的办公网络系统以及所有在办公网络上运行的信息系统。

1. **系统功能要求**

**4.1安全监测系统**

1. 为了节省资源和安全性考虑，要求采用全内置封闭式结构的1U机架式硬件设备。
2. 支持网卡限速，防止扫描消耗过多带宽。

4.1.1扫描运行在办公网络上的信息化设备：

* IP点授权（IP点数量）：授权可一次性扫描数量至少256个无限制范围的IP地址或域名；
* 主机漏洞数量大于等于9000个，web漏洞数量大于等于5000个，提供具有系统生产厂商盖章的证明
* 扫描类型（包括但不限于）：

1. 接入办公网络系统的信息化设备的安全漏洞。
2. 接入办公网络系统设备的安全配置问题。
3. 检查接入办公网络系统的设备中是否存在弱口令、弱密码。
4. 收集接入办公网络系统的设备有中不必要的开放的帐号、服务、端口等。
5. 扫描接入系统中设备的操作系统，收集操作系统的类型，版本号等。
6. 可以扫描出系统中私自架设的服务器，可具体定位到相应的信息化设备。
7. 扫描办公网络中各级交换机的相关安全配置(包括但不限于：端口信息配置、弱口令、弱密码、是否有安全漏洞等)。

* 风险等级：系统应在漏洞扫描过程中自动判断漏洞的风险程度，以不同的颜色提示管理者；
* 风险报告：根据扫描结果自动生成风险报告（网页形式），可以根据用户的要求自定义风险报告格式和输出内容，并且系统须根据漏洞类型和风险程度提出如何修补这些漏洞的建议；
* 生成的风险报告应包括但不限于以下几点：

1. 有风险的主机数量（根据不同的风险分类统计）。
2. 漏洞的数量（根据漏洞的风险分类统计）。
3. 漏洞风险分布统计（可以自定义柱状图、饼状图等）。
4. 系统中设备存在的弱口令、弱密码和无密码的设备数量
5. 主机扫描统计表（包括每台主机的漏洞数量和漏洞风险等级）。
6. 漏洞详细列表（里面包括漏洞类型、漏洞名称、漏洞危险等级、存在漏洞的主机数量和名称）。
7. 可利用漏洞提示，显示扫描出的漏洞是否可被利用。
8. 修补漏洞的详细方案（包括形成漏洞的原因和具体的解决方法）。

4.1.2扫描运行在办公网络上的信息系统

* 扫描类型(包括但不限于)

1. 收集运行在办公网络上的信息系统的安全配置信息。
2. 收集信息系统服务器操作系统和网站的类型和版本型号。
3. 扫描信息系统中存在的弱口令、弱密码。
4. 扫描系统服务器开放服务的端口和服务。
5. 扫描信息系统http及https协议的前端安全配置信息（是否SQL注入点、跨站脚本攻击点、WEBSHELL、上传漏洞等）

* 主动检查：通过扫描ip地址段，主动检查是否存在未报备的网站系统；
* 风险报告：根据扫描结果自动生成风险报告（网页或PDF形式），可以根据用户的要求自定义风险报告格式和输出内容，并且系统须根据漏洞类型和风险程度提出如何修补这些漏洞的建议，同时提供对这些扫描出的漏洞进行验证的方法；
* 生成的风险报告应包括但不限于以下几点：

1. 扫描的信息系统存在的风险漏洞（根据风险程度进行分类）。
2. 漏洞风险分布统计（可以自定义柱状图、饼状图等）。
3. 远程桌面弱密码检测，检测信息系统主机远程桌面开放情况，并记录存在远程桌面弱密码的主机情况。
4. 扫描信息系统的后端数据库的安全配置（数据是否会被恶意注入、修改、删除等）。
5. 数据库的的类型和版本号，以及数据库存在的安全漏洞。
6. 信息系统中相关设备存在的弱口令、弱密码和无密码的设备或虚拟服务器的IP地址。
7. 修补漏洞的详细方案（包括形成漏洞的原因和具体的解决方法）。

**4.2机房安全监测**

* 机房空调监测：包括空调运行状态、运行参数、空调管道是否漏水，并且可以使用系统远程控制空调的开关机，参数设置。
* 机房配电箱监测：监控配电箱的电流、电压的大小以及是否断电。
* 机房UPS监测：监测UPS是否正常工作，UPS是否能正常充电，当设备采用UPS供电时，UPS的电量数据。
* 机房内的温湿度监测：监测机房内温湿度的实时数据，要求机房内的监测点位部少于5个。
* 机房漏水监测：监测机房顶棚是否有漏水或冷凝水是否过多，顶棚不少于10个点位。
* 生成机房安全报告：

1. 机房日常巡检报告（包括：机房内空调运行情况、机房内的温湿度计，UPS电量以及是否有漏水情况）。
2. 如有设备故障需提供故障报告
   * + 1. 空调故障报告及其原因；
       2. UPS故障报告及其原因；
       3. 配电跳匝原因报告；
       4. 温湿度异常变化表。
3. 故障报告发送及时性，当系统发现故障时，5分钟内生成简易告警信息通过邮件或信息发送至机房管理员处，30分钟内于系统内生成完整故障分析报告。

**4.3系统适应性**

* 系统部署：支持单机单网络、单机多网络、分布式部署、扫描代理等多种接入方式，适应各种网络拓扑环境，同时需支持虚拟化镜像方式在虚拟环境下直接部署，支持IPv6网络环境下的部署和漏洞扫描；
* 系统更新：每个月对系统的安全漏洞库和检测规则进行更新，确保漏洞库和检测规则为版本最新；
* 系统影响：在系统扫描过程中不能对现有的办公网络系统造成任何影响（如长时间占用带宽，流量过大导致网络瘫痪，设备不能正常工作等）。
* 机房安全监测：要求能在断电、断网后继续运行，并按相关要求发送故障告警至机房管理员处。

**4.4配套硬件需求表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 物资名称 | 参考规格、技术参数及要求 | 品牌要求 | 单位 | 数量 | 使用部门/中心 | 备注 |
| 机房安全监测配套硬件 | 多路市电检测模块、UPS监控软件接口模块、精密空调监控软件接口模块、数字型温湿度传感器、漏水控制器、数据采集主机、纵横通综合监控平台软件V2.0、系统集成 | 纵横通、龙控、共济 | 套 | 1 | 企划部 |  |
| 远程安全监测系统配套硬件 | 含交流单电源，千兆电口6个。本次配置主机扫描模块。IP点授权（IP点数量），并发任务数≥5个，授权可扫描总数量不少于256个无限制范围的IP地址或域名 | 铱迅、绿盟、启明星辰 | 台 | 1 | 企划部 |  |

1. 注：设备包含安装、调试。
2. **系统咨询服务及培训**

**5.1信息安全咨询服务**

* 咨询服务：在质保期内每年不少于2次对招标方现有的信息系统安全管理工作提供咨询服务（包括但不限于：信息系统安全管理、专项培训、安全课件、宣传材料、网络攻防演练、黑客攻击等）；
* 文本咨询服务：在质保期内至少每年一次对《信息系统安全管理办法》提供咨询服务，提出文本中不能适应当前网络安全形式的问题和检测方法并以此提供最新的网络安全检测标准和检测方法；
* 生产性信息系统安全检查：在质保期内根据招标方的要求不少于每年2次配合招标方对《信息系统安全管理办法》内涉及的所有信息系统的文本及台账进行检查（含现场检查），要求按照相关等保要求提供检查方案和检查具体内容；
* 办公网络信息安全检查：在质保期内每年不少于4次，配合招标方对现有的办公网络系统进行安全检查，包括漏洞及分险扫描、台账检查、修复情况检查等；
* 信息系统安全检查：在质保期内每年不少于2次配合招标方对现有的运行在办公网络系统上的信息系统进行安全检查，包括漏洞及分险扫描、台账检查、修复情况检查等；
* 加固建议：供应商应在合同质保期内不少于每年2次配合招标方根据相关检查结果对办公网络及相关信息系统提供扫描修复及加固建议等解决方案或措施指导；
* 配合上级部门专项检查要求：配合招标方对上级部门（包括集团公司、交通运输委员会、公安网警等）专项安全检查提供相关的咨询和服务，如有需要应根据招标方的的要求提供上门应急支持，上门应急支持响应时间小于1小时，2小时内到达现场时间；
* 应急响应：在质保期内应确定专人对接相关信息系统安全服务并提供7\*24小时（需提供固定的联系方式，并24小时开机）相关远程安全支持和现场安全支持，包括：判断事件类型，并提供分析建议，查杀病毒，修补漏洞，追查来源，恢复系统，保留证据，并形成完整的信息系统安全报告。如要求现场应急服务响应时间应小于1小时，2小时内到达现场。
* 机房安全检查：在质保期内根据招标方要求每年不少于2次对机房安全检查，提供相关安全咨询服务和文本修订方案，并配合招标方对机房进行整改。
* 机房应急响应：在质保期内如机房发生安全问题，根据招标方要求派专业人员上门配合处理，要求响应时间小于1小时，2小时内到达现场。

**5.2 质保及培训**

* 质保期：系统供应商应提供两年的质保期并在质保期内须提供响应的支持和服务；
* 系统培训：供应商应在系统交付后提供所有相关文档并对信息系统安全管理人员进行系统使用培训，并在系统升级或软件更新后对新功能进行相应培训；
* 信息系统安全专项培训：供应商应针对信息安全领导小组、信息安全办公室、信息安全系统实际业务负责人员及一般员工分别制定对应的信息安全培训计划，每年不少于1次对相关人员进行专项信息安全培训；
* 信息安全专项培训考试：为招标方提供工信部认证的CISP高级网络安全工程师以及CCNP网络工程师各2人次培训及考试。
* 培训资料：根据招标方的要求提供相关信息安全培训的资料（包括但不限于培训文件、PPT、视频）；
* 提供培训的人员：提供培训的人员应具备相应的信息安全管理认证资质，由招标方审核通过方可进行培训。