

**网络安全服务调研问卷**

**河北中车数智科技有限公司**

**{{time}}**

目录

[1.基本信息 3](#_Toc7862)

[2.公网IP 3](#_Toc20739)

[4.网络分域情况 3](#_Toc27397)

[5.网络安全设备 3](#_Toc6834)

[6.人力资源 5](#_Toc8510)

[7.硬件资源 5](#_Toc24782)

[8.软件资源 5](#_Toc11444)

[8.1办公系统 5](#_Toc23728)

[8.2业务系统 6](#_Toc14179)

[8.3辅助系统 6](#_Toc13894)

[8.4外部对接系统 6](#_Toc24539)

[8.5外部业务系统 6](#_Toc14032)

[9.无线网络 6](#_Toc9093)

[10.辅助设备 6](#_Toc661)

[11.等级保护建设情况 7](#_Toc18441)

[12.网络安全服务情况 7](#_Toc6449)

[13.网络安全情报订阅情况 7](#_Toc9434)

[14.信息安全制度建设情况 7](#_Toc6511)

尊敬的客户：

为了更好地了解您的需求，提升我们为您提供的网络安全服务质量，请您协助填写以下问卷。感谢您的支持！

# 1.基本信息

**企业名称**： {{companyName}}

统一社会信用代码： {{socialCreditCode}}

所属行业： {{industry}}

上一年度营业收入： {{priorYearIncome}}

海外销售区域包括（国家）： {{overseasSalesArea}} ，分别的营业收入占比为 {{operatingIncomeRatio}}

**员工人数:**  {{employeesNumber}}

**联系姓名**： {{contactName}}

**联系电话**： {{contactMobile}}

**电子邮箱**： {{email}}

# 2.公网IP

是否云服务器： {{cloudServer}}

IP地址： {{ip}} 带宽： {{bandwidths}}

运营商：□联通 □电信 □移动 □教育 □广电 □阿里云 □腾讯云 □华为云

□亚马逊云 □微软云

# 3.网络拓扑图

是否存在网络拓扑图：{{networkTopology}}

附件一：网络拓扑图

# 4.网络分域情况

4.1单位是否划分了以下网络区域？

1.外网区： {{extranetArea}}

2.DMZ区： {{dmzArea}}

3.内网区： {{intranetArea}}

3.1 办公区： {{officeArea}}

3.2 运维区： {{operationArea}}

3.3 工业区： {{industrialZone}}

4.2单位使用的IP段及其用途（例如，10.10.10段用于办公，10.10.20段用于PACS设备等）：

{{ipSegment}}

# 5.网络安全设备

您所在单位是否使用以下安全设备？

1. 防火墙： {{isFirewalls}}

品牌：{{firewallsBrand}}

上线日期：{{firewallsDate}}

是否在保：{{isFirewallsInnocence}}

1. 数据库审计系统： {{isDatabaseAudits}}

品牌：{{databaseAuditsBrand}}

上线日期：{{databaseAuditsDate}}

是否在保：{{isDatabaseAuditsInnocence}}

1. 日志审计系统： {{isLogAudit}}

品牌：{{logAuditBrand}}

上线日期：{{logAuditDate}}

是否在保：{{isLogAuditInnocence}}

1. 堡垒机： {{isCitadel}}

品牌：{{citadelBrand}}

上线日期：{{citadelDate}}

是否在保：{{isCitadelInnocence}}

1. 态势感知： {{isSituational}}

品牌：{{situationalBrand}}

上线日期：{{situationalDate}}

是否在保：{{isSituationalInnocence}}

1. WAF： {{isWaf}}

品牌：{{wafBrand}}

上线日期：{{wafDate}}

是否在保：{{isWafInnocence}}

1. 漏洞扫描： {{isScan}}

品牌：{{scanBrand}}

上线日期：{{scanDate}}

是否在保：{{isScanInnocence}}

1. EDR： {{isEdr}}

品牌：{{edrBrand}}

上线日期：{{edrDate}}

是否在保：{{isEdrInnocence}}

1. 蜜罐： {{isPrivilegedEnv}}

品牌：{{privilegedEnvBrand}}

上线日期：{{privilegedEnvDate}}

是否在保：{{isPrivilegedEnvInnocence}}

1. 网闸： {{isInternetAccess}}

品牌：{{internetAccessBrand}}

上线日期：{{internetAccessDate}}

是否在保：{{isInternetAccessInnocence}}

1. 上网行为管理设备： {{isInternetDevice}}

品牌：{{internetDeviceBrand}}

上线日期：{{internetDeviceDate}}

是否在保：{{isInternetDeviceInnocence}}

1. 杀毒软件： {{isAntiSoftware}}

品牌：{{antiSoftwareBrand}}

上线日期：{{antiSoftwareDate}}

是否在保：{{isAntiSoftwareInnocence}}

1. 探针： {{isProbes}}

品牌：{{probesBrand}}

上线日期：{{probesDate}}

是否在保：{{isProbesInnocence}}

1. 其他（请注明）：

{{safetyOther}}

# 6.人力资源

请列出您所在单位现有的网络安全专业从业人员情况：

{{cyberSecurity}}

# 7.硬件资源

请列出您所在单位现有的硬件服务器设备及用途（例如，存储服务器、计算服务器等）：

{{hardwareRes}}

# 8.软件资源

请列出您所在单位现有的业务系统及用途：

# 8.1办公系统

（例如，OA办公、ERP、SAP等）：

{{officeRes}}

# 8.2业务系统

请列出您单位使用的业务系统（例如，客户关系系统、商城系统、服务客户业务系统等）：

{{businessRes}}

# 8.3辅助系统

请列出您单位使用的内网辅助系统（例如，系统维护系统、决策支持、物资管理、BI系统等）：

{{ancillaryRes}}

# 8.4外部对接系统

您单位是否对接以下外部系统？

传呼系统： {{pagingSystem}}

短信系统： {{messageSystem}}

环保系统： {{environmentalSystem}}

其他（请注明）： {{externalSystemOther}}

# 8.5外部业务系统

您单位是否提供以下对外服务系统？

门户网站： {{webPortal}}

互联网业务站点： {{internetBusinessSite}}

支付宝小程序： {{aliPay}}

微信小程序： {{wechatPay}}

微信公众号： {{wechatPublicNumber}}

其他（请注明）： {{externalSystemBusOther}}

# 9.无线网络

您所在单位是否提供无线局域网环境？ {{unlimitedNetwork}}

# 10.辅助设备

您单位是否使用以下联网辅助设备？

自助机： {{selfServiceMachine}}

扫码一体机： {{scanningMachine}}

PAD设备： {{padDevice}}

手持遥控设备： {{handheldDevice}}

其他（请注明）： {{ancillaryDeviceOther}}

如存在联网辅助设备，请列出具体设备名称：

{{ancillaryDeviceOtherEre}}

# 11.等级保护建设情况

您单位是否有系统做了等级保护建设？

①系统名称：

{{equalProtectionSystemA}}

②等级保护建设情况：

{{equalProtectionSystemADetail}}

①系统名称：

{{equalProtectionSystemB}}

②等级保护建设情况：

{{equalProtectionSystemBDetail}}

①系统名称：

{{equalProtectionSystemC}}

②等级保护建设情况：

{{equalProtectionSystemCDetail}}

# 12.网络安全服务情况

您单位是否聘请专业外部团队或内部团队定期进行网络安全相关检测，如渗透测试、代码审计、基线检查等。

如有，请填写：

{{cybersecurityServices}}

# 13.网络安全情报订阅情况

您单位是否订阅网络安全情报以能及时获取到最新漏洞情况。

如有，请填写:

{{cybersecurityServicesSub}}

# 14.信息安全情况

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 贵公司是否建立安全管理制度，包括对安全管理活动中的各类管理内容？ | {{secInfo1}} | {{asecInfo1}} |
| 2 | 贵公司是否有专人负责IT安全工作？ | {{secInfo2}} | {{asecInfo2}} |
| 3 | 贵公司是否有设定不同的安全岗位职责，如设定系统管理员、审计管理员和安全管理员等岗位？ | {{secInfo3}} | {{asecInfo3}} |
| 4 | 贵公司是否定期更新系统补丁？ | {{secInfo4}} | {{asecInfo4}} |
| 5 | 贵公司是否在物理安全区域（如机房，办公区）部署安防设备，如电子门禁系统、监控摄像头等？ | {{secInfo5}} | {{asecInfo5}} |
| 6 | 贵公司进出机房是否有相关管控措施（如需要提前审批或进行登记）？ | {{secInfo6}} | {{asecInfo6}} |
| 7 | 贵公司是否有清晰的管理员账户清单并且严格控制管理员权限？ | {{secInfo7}} | {{asecInfo7}} |
| 8 | 贵公司是否在网络边界处部署防火墙、IPS等设备防御网络攻击？ | {{secInfo8}} | {{asecInfo8}} |
| 9 | 贵公司是否部署抗DDoS设备，或采用抗D云防护服务？ | {{secInfo9}} | {{asecInfo9}} |
| 10 | 贵公司是否严格限制网络端口、通讯协议及系统服务？ | {{secInfo10}} | {{asecInfo10}} |
| 11 | 贵公司是否基于业务重要性或敏感性对网络进行分区管理（VLAN）？ | {{secInfo11}} | {{asecInfo11}} |
| 12 | 贵公司在网络边界的所有外部远程访问是否实现加密措施？ | {{secInfo12}} | {{asecInfo12}} |
| 13 | 贵公司信息系统中（服务器以及个人电脑）是否安装安全防护软件（如杀毒软件、终端防护、终端检测与响应、电子邮件网关等）？ | {{secInfo13}} | {{asecInfo13}} |
| 14 | 贵公司是否有对重要业务数据进行定期备份，并定期维护和测试这些备份数据的有效性？ | {{secInfo14}} | {{asecInfo14}} |
| 15 | 贵公司是否在终端部署软件对USB和其他外设的使用进行监控，防止未知USB接入系统？ | {{secInfo15}} | {{asecInfo15}} |
| 16 | 贵公司是否建立人员离岗管理制度，在员工离职后是否能够及时终止离岗人员的所有访问权限，取回所有安全相关的硬件设备？ | {{secInfo16}} | {{asecInfo16}} |
| 17 | 贵公司针对安全团队是否有定期(每年至少1次)提供安全技能培训，如网络攻防、安全操作和维护等？ | {{secInfo17}} | {{asecInfo17}} |
| 18 | 贵公司针对公司全体员工是否有定期(每年至少1次)提供安全意识教育培训？ | {{secInfo18}} | {{asecInfo18}} |
| 19 | 贵公司是否通过相关信息安全管理体系认证(ISO 27001)？ | {{secInfo19}} | {{asecInfo19}} |
| 20 | 近一年内，贵公司的重要信息系统是否通过等级保护测评？ | {{secInfo20}} | {{asecInfo20}} |
| 21 | 贵公司针对电子邮件是否采取安全防护措施，如反垃圾邮件网关、沙箱等？ | {{secInfo21}} | {{asecInfo21}} |
| 22 | 贵公司是否集中监控和管理信息系统的计算和存储资源，确保其资源满足业务高峰期的需要？ | {{secInfo22}} | {{asecInfo22}} |

感谢您的时间和支持！我们将根据您提供的信息为您制定更为精准的网络安全解决方案。

如果有其他问题或需要进一步的帮助，请随时联系我们。

联系邮箱：565325162@qq.com

联系电话：13731517922