网络等保2.0基本要求有哪些

产品名称	网络等保2.0基本要求有哪些
公司名称	上海道商企业服务中心
价格	.00/个
规格参数	
公司地址	浦东新区金沪路99弄3号
联系电话	15021594806 15021594806

产品详情

等保2.0相对1.0的变化 等级保护2.0中将整体结构进行调整，从物理安全、网络安全、主机安全、应用安全、数据安全变成安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心，所以原等级保护1.0中的「网络安全」变成「安全通信网络」。 等保2.0基本要求有哪些
结构安全对企业、安全厂家、系统集成商提出的要求： 1)企业或集成商进行网络基础建设时，必须要对通信线路、关键网络设备和关键计算设备进行冗余配置，例如关键网络设备应采用主备或负载均衡的部署方式; 2)安全厂家在进行安全解决方案设计时，也应采用主备或负载均衡的方式进行设计、部署; 3)强调、突出了网络区域的概念，无论在网络基础建设，还是安全网络规划，都应该根据系统应用的实际情况进行区域划分。 访问控制对企业、安全厂家、系统集成商提出的要求： 1)要着重考虑网络边界的访问控制手段，但网络边界不仅仅是业务系统对其他系统的网络边界，还应该包括在业务系统内不同工艺区域的网络边界; 2)访问控制的颗粒度要进一步的强化，不仅仅要停留在对于HTTP,FTP,TELNET,SMTP等通用协议的命令级控制程度，而是要对进出网络数据流的所有应用协议和应用内容都要进行深度解析; 3)企业用户在进行网络安全防护项目招标时一定要考虑参与投标的安全厂家所采用的边界访问控制设备是否具备对应用协议深度解析的能力，例如在工业控制系统，除了能够对比较常见的OPC、ModBusTCP、DNP3、S7等协议进行深度解析外，还需要根据现场业务实际情况，对业务系统中使用的私有协议进行自定义深度解析，否则很难达到测评要求。 安全审计对企业、安全厂家、系统集成商提出的要求： 1)重点强调了需要在网络边界、重要网络节点处进行网络行为审计，要求企业在进行网络安全防护项目时要充分考虑网络边界和重要网络节点的行为审计能力，例如在城市轨道交通信号系统中，车站分为一级集中站、二级集中站和非集中站，结合等级保护2.0的要求，需要在一级和二级集中站都要考虑部署具备网络行为审计能力的安全产品。而仅仅在一级集中站内部署具有网络行为审计能力的产品是不够的。 2)重点强调网络行为审计，即对网络流量进行审计，而这仅仅靠原有的日志审计类产品是不够的，无法满足等级保护2.0的要求。 边界完整性&入侵防范&恶意代码防范对企业、安全厂家、系统集成商提出的要求： 1)对于企业和系统集成商，在进行网络安全防护项目招标时要充分考虑对于在等级保护2.0中所提出的对于「已知」和「未知」的检测要求。尤其在进行安全厂家选择时，要重点考虑安全厂家对于「未知」攻击的检测能力; 2)对于安全厂家，网络安全审计或入侵检测产品不应仅仅局限在采用「特征库」的形式进行攻击检测，因为采用以「特征库」为模板的形式无法对「未知」攻击进行检测; 3)对于安全厂家，入侵防范的范围变化，需要在网络安全解决方案设计时充分考虑，不应仅仅在网络边界处进行入侵防范，还需要在网络中的关键节点处均需要进行入侵防范。 等保2.0三级基本要求：
身份鉴别对企业、安全厂家、系统集成商提出的要求： 1)集成商进行业务应用软件设计时，应考虑业务应用系统在「用户名」+「口令」的基础上进一步实现通过密码技术对登录用户的身份进行鉴别，同时

应避免业务应用系统的弱口令问题;
2)集成商进行业务应用软件设计时，应充分考虑用户权限的控制以及用户在登录失败后的处理机制; 3)企业在业务运营期间不可通过不可控的网络环境进行远程管理，容易被监听，造成数据的泄露，甚至篡改; 4)安全厂家在进行安全产品选用时，应采用具有两种或以上的组合鉴别方式的安全防护软件对登录系统的管理用户进行身份鉴别。满足本地身份认证和第三方远程身份认证双因子验证要求。
访问控制对企业、安全厂家、系统集成商提出的要求： 1)集成商进行业务应用软件设计时，应充分考虑用户权限的控制以及用户在登录失败后的处理机制，确保业务应用系统不存在访问控制失效的情况; 2)企业或集成商在进行系统配置时，应为用户分配账户和权限，删除或重命名默认账户及默认口令，删除过期、多余和共享的账户; 3)安全厂家在进行安全产品选用时，应采用符合强制访问控制要求的安全防护软件对主机、系统进行防护，可以有效的降低高风险项的风险等级。
安全审计对企业、安全厂家、系统集成商提出的要求： 1)对集成商而言，业务应用系统软件的安全审计能力至关重要，需要能够对重要用户操作、行为进行日志审计，并且审计的范围不仅仅是针对前端用户，也要针对后端用户; 2)对企业来说，在基础建设时应该在重要核心设备、操作系统、数据库性能允许的前提下，开启用户操作类和安全事件的审计策略，并在安全运营的过程中对策略的开启定期检查; 3)安全厂家在进行安全审计产品选用时，应采用可以覆盖到每个用户并可对重要的用户行为和重要安全事件进行审计的产品。可利用日志审计系统实现对日志的审计分析并生产报表，通过堡垒机来实现对第三方运维操作的审计。 剩余信息保护对企业、安全厂家、系统集成商提出的要求：
企业或集成商在服务器上启用基于操作系统本身的剩余信息保护功能。
入侵防范对企业、安全厂家、系统集成商提出的要求：
1)企业或集成商在进行系统安装时，遵循小安装原则，仅安装业务应用程序及相关的组件; 2)企业或集成商进行应用软件开发时，需要考虑应用软件本身对数据的符合性进行检验，确保通过人机接口或通信接口收到的数据内容符合系统应用的要求; 3)企业或集成商在选择主机安全防护软件时除了要考虑主机安全防护软件的安全功能以外，还要考虑与实际业务场景结合的问题，能够有效的帮助业主解决实际痛点。工业现场大部分现场运维人员对安全知之甚少，很难严格按照等级保护要求将安全配置一一完善，所以选择的主机安全防护软件应可以通过简单的配置来满足等级保护的要求; 4)解决安全漏洞直接的办法是更新补丁，但对于工业控制系统而言，打补丁的动作越谨慎越好，避免由于更新补丁而影响到生产业务。该条款需要企业委托第三方工控安全厂家对系统进行漏洞的扫描，发现可能存在的已知漏洞，根据不同的风险等级形成报告，企业或集成商根据报告在离线环境经过测试评估无误后对漏洞进行修补。
恶意代码防范对企业、安全厂家、系统集成商提出的要求： 工业现场恶意代码防范一直是用户的痛点，受制于工业现场环境，杀毒软件无法在工业环境内发挥作用。误杀、漏杀、占用资源、无法升级等问题一直被诟病。所以在工业场景中应该选择采用白名单机制的安全防护软件。
资源控制对企业、安全厂家、系统集成商提出的要求： 在工业现场大部分的场景对于数据传输、存储完整性要求要高于数据传输、存储保密性要求。对于系统集成商在应用通过密码技术来保证传输数据的完整性，并在服务器端对数据有效性进行验证。 在工业现场关键服务器、工作站内存储的业务软件及配置文件的完整性和可用性是至关重要的，一旦其完整性遭到破坏，直接影响现场生产任务。所以对于安全厂家提出的要求就是其安全防护软件应可以通过访问控制功能，对存储的数据、配置文件进行完整性保护，避免遭到非法破坏。
企业应建立异地备份中心，同时形成数据备份制度，定期进行现场的关键数据、配置文件的备份。