

信息网络等级保护解决方案

为了加强对国家信息系统的保密管理,确保信息安全,国家明确提出了信息系统的建设使用单位必须根据分级保护管理办法和有关标准,对信息系统分等级实施保护。

2007年,公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合发布了《信息安全等级保护管理办法》。《办法》将信息系统的安全保护等级分为以下五级:

- 第一级,信息系统受到破坏后,会对公民、法人和其他组织的合法权益造成损害,但不损害国家安全、社会秩序和公共利益。
- 第二级,信息系统受到破坏后,会对公民、法人和其他组织的合法权益产生严重损害,或者对社会秩序和公共利益造成损害,但不损害国家安全。
- 第三级,信息系统受到破坏后,会对社会秩序和公共利益造成严重损害,或者对国家安全造成损害。
- 第四级,信息系统受到破坏后,会对社会秩序和公共利益造成特别严重损害,或者对国家安全造成严重损害。
- 第五级,信息系统受到破坏后,会对国家安全造成特别严重损害。

军队、军工和政府等网络中存有大量敏感信息,需要进行强制保护,因此有必要基于等级保护和分级管理制度进行内部网络建设,增加网络的分域和分级管理水平,确保不同等级的信息系统的有效隔离和保护。

● 安全风险分析:

- 1) 内部网络和外网应相互隔离,包括网络设备和移动存储介质在内不应相互连接,不允许将存有涉密数据和信息的存储介质在非涉密网计算机上使用;
- 2) 内部网络根据信息系统保密等级的不同,要进行逻辑隔离,分域分级管理,实行分等级保护;
- 3) 不同保密等级的信息系统,应采用不同的防护措施;



- 4) 未经管理人员同意, 不能将内部信息系统中的任何数据带出内部管理范围;
- 5) 不能将任何非涉密设备接入涉密信息系统;
- 6) 两个不同的计算机网络, 即使具有相同等级的安全级别, 没有管理员特别批准, 也不能互联互通;
- 7) 内部信息系统中的数据, 要带离该网络, 必须经过管理员审批;
- 8) 对内部移动存储介质(如U盘)等必须采取有效的管理措施。

● 解决方案:

中安源可信网络安全平台, 通过在内网中划分“安全域”的方式实现了内部网络的分域分级管理, 所有的内网主机按照职能和级别不同被划入不同的“安全域”中进行管理, 隔离外来的计算机, 并提供移动存储介质的授权和保密管理。中安源可信网络安全平台解决了通信安全、访问控制、移动存储介质管理和数据存储安全等可能导致网络内部信息泄密的问题。

- 1) 以身份认证为基础, 以数据安全为核心, 以监控审计为辅助, 基于网络加密和存储加密技术, 解决内部网络安全问题, 提高整个网络的分级分域管理水平;
- 2) 根据等级保护的技术标准, 可以将内部网络信息系统的计算机终端和服务端根据行政区域、保密级别和部门等的不同, 划分成不同的安全域, 进行分级分域管理;
- 3) 同一个安全域内的计算机可以相互之间进行正常的网络通信和以存储介质为载体的数据交换, 但是不同安全域之间, 未经管理员允许, 不能通过任何方式进行数据交换;
- 4) 自动对网络上传输的数据进行加密保护, 可有效防止网络上非法窃听行为的发生, 非法用户无法在网络上窃取信息;
- 5) 对数据存储途径进行了全面保护, 对移动存储介质存储提供了基于文件的自动加密存储功能;
- 6) 通过网络加密技术, 彻底杜绝了各种方式的非法外联和非法接入, 包括计算机对等网的连接方式;

- 7) 可以实现对计算机外部设备的统一控制和管理, 防止因为外来设备接入带来的安全隐患;
- 8) 提供了完善的移动存储介质(U盘等)管理技术, 可以支持多种灵活的策略和授权方式, 实现内部移动存储介质的统一管理;
- 9) 提供了详细的审计记录, 并可以提供定制化的报表;
- 10) 根据用户要求, 可以提供高强度的身份认证措施, 基于 USB 令牌或者指纹识别器。

● 系统部署示意图:

