论企业信息系统的安全

摘要

我公司是一家专门从事集装箱装卸业务的码头公司。随着公司业务的发展和生产管理的需要，公司建立起了一套比较全面的信息系统，该系统涉及到生产控制、计费、客户服务、财务、人力资源、办公自动化、设备管理、物资采购等多个方面，作为公司 IT 部门的负责人，我负责公司信息系统的规划、建设、运行管理、升级维护的整个过程。

为了确保公司信息系统的安全，我们从系统的规划、建设阶段到系统的运行维护阶段整个过程都把系统安全作为一项重要的工作来抓，从硬件、系统软件的选用、网络结构的设计、应用软件的设计、开发，到服务器、客户端的日常管理都制定了系统安全相关的规范和制度，并严格执行，多年来，公司的信息系统运行稳定，确保了公司生产管理的顺利进行。

正文

我公司是一家专门从事内外贸集装箱装卸业务的集装箱码头公司。随着公司生产发展和管理的需要，公司已经建立起了一套比较全面的信息系统，主要包括船舶作业控制、堆场作业控制、商务计费、客户服务网站和 EDI 系统、财务、人

力资源管理、办公自动化、设备管理、物资采购等多个系统，其中，生产管理系统、客户服务网站和 EDI 系统必须 24 小时稳定运行，指挥和控制公司的堆场和码头作业，并向客户提供及时、准确的信息服务，其他系统也对信息的安全性和系统的稳定运行有非常高的要求，公司对 IT 部门有严格的考核指标。

为了确保公司信息系统的安全，我们从系统的规划、设计阶段到系统的运行维护阶段整个过程都把系统安全作为一项非常重要的工作来抓。通常，在企业信息系统中，必须要考虑硬件安全、网络和系统的安全以及数据安全问题：

1、硬件安全

硬件安全是系统安全的第一道关口，机房防火、防雷击、防故意或者无意的破坏等；采用可靠的硬件设备，防止设备内置窃听装置和功能等；网络线路和设备的物理安全、运行环境的安全等都是企业信息系统安全需要考虑的因素。

2、网络和系统的安全

网络和系统安全的目的是要确保企业网络系统能够按照预先设定的权限范围访问，内网和外网之间不能进行超出范围的访问，内网的各个子网之间，各台电脑之间都要在限定的权限范围内进行访问，服务器和客户端电脑本身和用户之间也要在限定的权限范围内访问；能够抵御非法的攻击和病毒的侵扰等。

3、数据安全

数据安全主要涉及到数据的合法访问、数据保存期内不能丢失等要求。企业

的信息系统一般都有严格的访问权限，数据的查询、增加、修改、删除等都有严格的权限管理，必须要确保数据的合法访问。同时，企业数据必须考虑到防止丢失，防止媒体故障、损坏和灾难造成数据丢失等。

根据我公司的特点，我们在信息系统的安全方面主要采取了以下解决方案：

1、严格、全面的安全管理制度和执行力

在系统安全方面，我们认为，首先是思想上要重视，要让公司领导、管理人员、操作人员都重视信息系统的安全，工作开展才会比较顺利。我们制定了严格、全面的信息系统安全管理规定，并利用一切机会向有关人员说明系统安全的重要性，得到了公司领导和使用人员的理解和支持，安全规定得以比较严格地执行。

2、硬件安全方面

我们认为，硬件安全是系统安全的第一道关口。所以，我们严格机房的建设和管理规范，采取严格的防火、防雷击、双回路 UPS 供电等措施，对进入机房的人员进行严格管理。网络方面，网络线路尽可能进桥架、管道，注意设备的安装环境，特别是室外设备物理安全、供电安全等。

客户机方面，我们将客户端机箱贴封条，禁止私自打开机箱安装硬件、改变 CMOS 设置等，为防止用户使用 U 盘、手机上网等，我们将重点岗位电脑的端口（USB 端口、读卡器）尽可能封闭，不安装光驱，用网络打印机取代 USB 接口打印机等，使用户无法自己改变电脑配置。

3、网络和系统的安全

采用防火墙将将公司的内外网进行隔离，只开放需要的端口，其他的一律关闭，并设置了防止端口扫描、入侵检测等防攻击手段。

通过 IP 地址和交换机端口的绑定，用 IP 地址控制部分系统权限。内部设置 VPN，按照部门和使用功能需求，尽可能缩小 VPN 范围，防止类似 ARP 类型的病毒通过大量发送广播包影响网络，也防止互相之间通过共享安装软件和拷贝数据等。

用户名和密码管理，服务器原则上只设系统管理员用户（两名系统管理员共用），不设其他用户。客户端尽可能少设用户，并且对客户权限进行限制。

公司内部服务器和客户机的上网进行了严格的控制，服务器原则上不允许上网，所有系统软件的补丁都通过专门的补丁服务器下载到内部网，经过确认后再安装到电脑上。对于 EDI 服务器等必须通过互联网和外部服务器连接的，也采用防火墙对服务器的端口进行严格管理，只开放必须的端口；客户端的电脑严格控制上网，能不上网的不上网，必须上网的也通过代理服务器对目的网址、协议、端口等进行严格控制。

公司所有的电脑都安装了网络版的防病毒软件，为了确保效果，我们公司分不同的电脑，采用了两套网络版的防病毒软件，统一升级和定期扫描病毒。

我们将客户电脑的“我的文档”、电子邮件文件等所有用户文件都放在 C 盘

以外的路径，封锁用户对 C 盘的使用权，车载电脑等不需要用户自己数据的系统硬盘全部封锁，并采用影子系统，每次开机自动恢复系统。

严格共享信息的管理，通过域服务器统一认证身份，指明共享用户范围。

4、数据安全方面

严格控制数据库服务器管理员密码。应用软件对数据库的访问采用二级密码控制，应用软件先通过一个经过加密的“预用户 ”访问数据库服务器，“预用户 ’用户权限非常小，只能读取经过加密的正式用户的用户名和密码，在解密后再次连接才能正式使用数据库，这样做确保了客户端不保存数据库正式用户的任何信息，而且管理人员可以随时更改数据库用户的密码。

严格应用软件的使用权限，人力资源部人员岗位变动后，直接修改操作员权限。

敏感数据加密存放，防止包括系统开发或者管理人员未经许可的访问。禁止开发人员和系统维护人员直接对数据库的操作。尽量详细的应用程序操作日志和系统日志。

采用多级数据备份，实时备份，定期冗余备份相结合。

通过采用了上述措施，基本上保障了我公司的信息系统的安全运行，我公司的信息系统运行多年来，从未出现过大规模地病毒爆发、系统瘫痪、数据丢失或被窜改等灾难事件。

客观地说，我公司的信息系统还存在一个比较大的安全隐患，就是异地备份问题，由于费用的考虑和条件的限制，加上这种灾难的概率非常的小，目前我们还没有建立异地备份系统。好在我们公司目前正在进行二期集装箱码头的建设工程，在二期工程的设计中本来就有一个比较大的弱电间，我们已经向设计院建议按照标准机房的要求来设计和建设，以便在二期工程中建设备份系统。

另外，随着互联网功能的越来越丰富，企业内部对于互联网的使用需求也越来越多，随之而来的是互联网上的恶意插件、病毒的威胁也越来越大，为了尽可能地利用互联网为公司的经营管理服务，我们也不得不在系统安全和更大的需求之间平衡，这无意增加了内部系统的不安全因素，但是，我们坚持核心的生产控制系统不能连接互联网，确实需要上网的地方，就增加独立的外网电脑，以确保系统的安全运行。

信息系统的安全是一项长期的工作，需要我们不断地学习新技术、不断地积累和借鉴经验，并及时付诸实施，才能确保信息系统的安全。