文章编号:1000 - 582X(2003)07 - 0042 - 05

# 制造企业信息集成平台安全性现状及其对策*

王 成 良
(重庆大学 软件学院,重庆 400044)

**摘 要**:制造企业信息集成平台是一个支持复杂信息环境下应用开发、应用集成和系统运行的软硬件平台,企业的信息化依赖于这个信息集成平台。当前计算机安全性问题较为突出,因此如何保证制造企业信息集成平台的安全性是一个值得重视的问题。介绍了当前制造企业信息集成平台安全性的现状问题,提出了企业在信息化过程中应该采取的安全措施。重点指出了将安全管理制度与安全管理技术结合起来,整个企业信息集成系统的安全性才有保证。

**关键词**:制造企业; 信息集成平台; 计算机安全性
**中图分类号**:TP393.08　　**文献标识码**:A

在制造企业信息集成平台中,存在着异构计算机平台、异构网络平台、异构操作系统、异构数据库平台、不同的 WEB 服务器和邮件服务器、FTP 服务器以及各类系统工具软件和应用软件,其中应用软件包括各类 CAD/CAPP/CAM 软件、PDM、MRPII、ERP、MIS、CAQ 等。这是一个非常复杂的信息集成平台[1],涉及到生产制造过程中的方方面面,包括产品设计、工艺设计、加工制造、质量检验、网上订货、网上销售、办公管理、网络化制造等。威胁到企业信息集成平台安全性的主要动机来自以下几个方面:

1)网络入侵者为了获得巨额报酬而受雇于某人或某企业,攻入企业网络盗窃或篡改信息;

2)入侵者闲极无聊又具有一定的计算机知识,因此总想对网络进行点什么处理才好;

3)入侵者非常熟悉计算机,想通过攻入大家都认为很难渗入的区域来证明他的能力,而攻击成功可以让攻击者得到同类的尊敬和认可;

4)入侵者被停职、解雇、降职或受到某些不公正的待遇,转而进行报复,对网络进行破坏或利用不严格的访问控制措施,窃取企业网中的重要技术资料或破坏服务器中保存的重要信息;

5)入侵者正在学习计算机和网络,无意中发现的一些弱点可能导致数据被毁或执行非法操作;

6)由于企业内部个人之间的恩怨而一方想尽办法攻击另一方的计算机,使之瘫痪而后快。

总之对制造企业信息集成平台造成安全威胁的动机各式各样,在网络安全和信息安全日趋严重的当前,必须从战略的高度来考虑整个企业信息集成平台的安全性。

## 1 制造企业信息集成平台安全性现状

随着我国 863/CIMS 示范工程的实施,不少制造企业都已经建成了企业内部网,实现了信息孤岛之间的集成,并且正在朝着并行集成、企业集成的方向迈进。在企业的信息集成平台中,以光纤和双绞线以及同轴电缆通讯介质,建立了企业计算机骨干网络以及各个子网,使位于企业不同地理位置的部门或单位融合于统一的企业内部网中。一级主干网实现了各个分系统的信息集成和 Internet/Intranet 接口网络环境,二级子网用于实现各个单元技术的网络环境。在一级主干网中已经采用 100 Mbps 的快速以太网交换技术,在二级子网中采用了 10 Mbps 或者 100 Mbps 的以太网交换或共享技术。在网络协议上一般采用了 TCP/IP 和 NETBEUI 协议;在网络设备选型上采用了交换机和集线器产品,充分考虑了网络系统的可靠性、可维护性、设备兼容性和扩展性。在应用软件上引进和自主开发或合作开发了各类应用软件,包括产品数据管理 PDM 软件、MRPII 软件、ERP 软件、MIS 软件、各类 CAD/CAPP/CAM 软件等,建立了 Intranet 环境下信息集成管理系统。在企业信息集成平台中初步实现了硬件资源、软件资源、数据资源的共享,使得企业的运作效率大大提高[2-4],缩短了产品设计开发、制造周期,提高了产品质量,取得较大的经济效益。

* 收稿日期:2002 - 09 - 11;修改稿收到日期:2003 - 03 - 09
基金项目:重庆市应用基础研究项目(20016809)
作者简介:王成良(1964 - ),男,江苏丹阳人,重庆大学博士,副教授,主要从事网络及数据库应用技术研究。

由于这种应用还属于初步阶段，因此对企业内部的信息集成平台的安全性考虑较少，甚至没有实质性的要求。随着企业越来越依靠信息系统，人们对提高信息集成平台的安全性的要求也逐步提高，特别是近年来有关网络安全的漏洞或失误所造成破坏的不断出现和报道，使得信息集成平台的安全性成为人们必须直面的一个问题。

企业内部信息集成平台由于用户多、资源共享程度高，因此所面临的威胁和攻击是错综复杂的，企业内部网入侵者不但会想办法窃取、篡改网上的机密信息，还可能会对网中的设备进行攻击，使企业内部网设备瘫痪。为了保护企业信息内部网信息的机密性、维护信息的完整性、减少病毒感染、保护企业内部网设备，就必须控制对企业内部网资源的访问。企业内部网中常见的不安全因素有以下几个方面：

1）企业内部网操作和控制系统的复杂性妨碍了对企业内部网安全的确认；

2）企业内部网必须面对多个用户的访问；

3）企业内部网具有未知的边界，企业内部网服务器可能与一些它不知道的用户存在潜在的连接；

4）可能存在着多点攻击和攻击手段的多样性；

5）用户对企业内部网服务器的访问可能存在多条路径，而有些未知路径会存在安全隐患。

上述不安全因素具有一般性原则。目前制造企业信息集成平台大致存在着以下几个方面的安全性问题。

### 1.1　网络规划设计不尽合理，网络布线不规范

企业在网络建设初期，出于资金方面的考虑，没有从总体安全性方面考虑，网络综合化布线不符合国家《建筑与建筑群综合布线系统工程设计规范》；在网络规划设计时，没有从整个企业各个部门之间的网络访问控制方面进行考虑，使得后续实施网络安全访问控制时带来不便。例如将整个企业的内部 IP 地址归属于同一个网段，使得不管哪一级使用人员都可以从“网上邻居”去探寻点什么。

### 1.2　网络操作系统中的补丁包没有及时升级

操作系统是计算机系统中的一个系统软件，它能有效地组织和管理计算机系统中的硬件和软件资源，合理地组织计算机工作流程，控制程序的执行，并向用户提供各种服务功能，使得用户能够灵活、方便、有效地使用计算机、使整个计算机系统能高效地运行。但操作系统的开发是一项浩大的工程，系统在投入使用后由于设计方面的有意或无意的原因，难免存在着一些缺陷（Bug），有些甚至是严重的安全漏洞，在人们逐步发现以后，软件开发商一般都会提供升级补丁包。例如微软公司在 1997 年发布的 Windows NT 4.0 操作系统中，就存在着较多的网络安全和信息安全漏洞，随着人们应用的增多，在逐步发现之后，微软已作了相应的升级处理，以 Service Pack 包的发行方式发行。但由于企业的信息系统一直运行良好，觉得没有必要升级，忽视了潜在的网络安全和信息安全漏洞，从而造成系统安全漏洞。

### 1.3　系统登录问题

在制造企业的信息集成平台中，系统登录问题没有引起人们的足够重视。例如很多网络工作站采用 Windows95/ Windows98/ Windows Me 等作为桌面操作系统，采用 Windows 网络登录方式，输入用户名和口令可以登录网络，以为不知道口令虽然可以进入系统但无法登录网络，觉得有安全性保障。实际上虽然通过网上邻居无法查看网络，但由于加载了 TCP/IP 网络协议，仍然有很多方法进入网络，例如直接在安装了 Active Desktop 的资源管理器的地址栏，输入某个网络计算机的共享目录，例如“\quality - 1\c\tools”，其目录内容就会马上显示在你的计算机上，而且可以进行其它相关操作。

### 1.4　口令问题

企业用户在登录系统时，一般都要输入登录口令，网上资源的共享也需要口令才可以具有访问的权限。但由于人们习惯于使用自己或家人及朋友的生日和使用自己的姓名或家人的姓名，甚至于键盘上的单个或两个字符等作为口令，这些口令很容易被别人猜测到，因此存在着较为严重的安全性问题。

### 1.5　网络中对资源的访问权限的控制

对于整个企业中哪些人该访问网络中的哪些资源或不应该访问网络中的哪些资源没有很好地进行规划和设计，随意性比较大。对于重要部门，当某人需要使用打印机时，可能要求系统管理员将打印机共享，打印完毕后系统管理员忘记了取消打印共享，可能造成重要资料的打印泄漏。有些人本来只能访问其工作范围内的网络计算机，但由于疏漏却可以越过某些安全检查，访问到其它网络计算机，从而对安全造成隐患甚至威胁。

### 1.6　拨号上网问题

企业某些部门为了通过电子邮件方便对外联系，查询信息，购买了调制解调器用于拨号上网，而可以拨号上网的计算机就连接在企业内部网上，它是企业内部网上的 1 台网络工作站，这样就为企业信息集成平台的安全打开了一条后门，随电子邮件带回的病毒可以对网络系统造成感染。网上黑客通过 BO 后门程序在监视你的行动，也可能造成企业重要信息的泄漏。

### 1.7　重要电子文档和资料安全问题

为了实现整个企业的信息共享，在企业内部网中存放了各种重要的办公文档、图纸、工厂资料等，这些文档和资料作为文件存放在各个目录下，没有进行统一的管理，没有经过加密处理，仅仅通过共享访问口令进行目录的访问控制。实际上通过共享口令访问很容易被解破[5]。另外虽然可以通过 Microsoft Word 以及 Microsoft Excel 等对文档进行口令保护，但很容易被解破。

### 1.8 服务器系统的配置方面的安全性问题

许多制造企业建成了自己的 Intranet 内部网，主要目的在于沟通信息孤岛，使企业各部分工作能在一个方便的平台上很容易地共享企业信息资源，特别注重为决策和管理层领导提供管理决策所需的信息服务，服务器系统采用了 Web 服务器、邮件服务器、FTP 服务器等等，在建立这些服务器的时候，由于每一样服务器的配置比较复杂，精通的人又比较少，因此满足于能够用起来，一般采用了系统的默认配置。实际上在这些默认配置中，对安全性方面考虑较少。例如基于 Windows 2000 Advanced Server 中的 IIS(Internet Information Server) Web 服务器配置中，采用默认配置后，在客户端通过浏览器可以看到 global. asa 文件中的所有内容，而该文件正是 Web 站点的关键文件，里面存放了数据库的访问口令等重要数据。同样在 Microsoft Exchange Server 2000 邮件服务器中按默认配置的话，则网络黑客可以使你的邮件系统不能正常工作，最后不得不放弃原有的邮箱数据，重新安装。FTP 服务器配置不当的话，容易遭到攻击，将许多无用的文件上传到服务器上，直到你的服务器硬盘物理空间消耗殆尽，最终使系统瘫痪。

### 1.9 存在数据库安全性方面的问题

制造企业信息集成平台中，数据库系统是整个企业数据信息的中心。数据存放到数据库后，就可以对各类数据进行科学管理。但恰恰在管理过程中存在着安全漏洞。例如数据没有经过加密就保存到 Foxbase、Foxpro、visual Foxpro 等数据库中，很容易被非法用户访问而造成数据的泄漏。在 Microsoft Access 数据库中，可将数据存放在数据表中，虽然对数据库加了口令，但目前口令解密的工具唾手可得。对于大型数据库如 Microsoft SQL Server 、Adaptive Sybase 、informix、IBM DB2、Oracle 等，虽然它们功能强大，都有一套自己的数据库安全保护机制，但如系统配置不当就会造成安全隐患。例如在 Microsoft SQL Server 7.0 中，如果开启远程访问功能，当数据库服务器和 WEB 服务器同装于一台机器上时，借助于 Internet 可获得数据库服务器的 IP 地址，通过远端机的 SQL Server 7.0 的 Enterprise Manager 可建立起一个管理对象，而登录数据库的口令可通过前面介绍的 Global. asa 文件查看得到，这样你的数据库就会完全被别人控制。

### 1.10 应用软件的安全性问题

应用软件在开发过程中由于原先对安全性方面的考虑较少，造成现有的一些应用软件存在安全性问题。例如对于一些重要数据的应用程序保护方面，没有做到操作留痕迹的日志功能，一旦出现安全问题，无从查找；用户在登录进入应用程序后，就再也没有任何约束限制，可自由操作；对数据库的操作权限在程序中没有进行控制；数据写入数据库中时没有考虑加密处理；

### 1.11 企业内部网的安全问题

企业内部网和 INTERNET 之间没有进行有效的安全隔离；企业内部网的子网与子网之间没有进行有效的安全隔离。直接通过 ISDN、DDN、ASDL、Ethernet 连接于 Internet 的企业，没有购买必要的防火墙；即使购买了防火墙，可能没有进行精心合理的配置，造成安全漏洞。企业的各类二级子网应以部门为单位或以业务紧密联系的部门为单位来构造，子网中的用户要访问主干网中的信息可能没有通过代理服务器进行 IP 过滤，造成了子网上的用户可以随便访问主干网上计算机。

### 1.12 没有安装必要的病毒防火墙软件

计算机病毒的危害是巨大的，它可以破坏数据、使系统瘫痪、损坏硬件，使系统工作不稳定。一般通过软盘或光盘中的软件以及电子邮件、网页来感染计算机系统。如果说，软盘或光盘中软件病毒的感染，可通过不安装软盘驱动器和光盘驱动器解决的话，则从电子邮件和网页传送来的病毒是最大的祸害和根源。网络版的病毒防火墙服务器可以对下载的文档进行解毒处理，可以自动清除邮件病毒，对杀不死的带病毒邮件退回原发送人。但很多单位从节约资金出发，没有购买网络版的病毒防火墙服务器，因此一旦病毒进入企业内部网，损失不言而喻。

### 1.13 对重要文件和数据的备份不够重视

备份是唯一能够快速恢复系统平台运行的法宝。备份包括几个方面的层次，例如磁带备份、光盘备份、冗余磁盘阵列备份、双机备份、双机热备份、远程数据备份等等。有些制造企业对数据备份重视不够，例如关键的数据没有天天按时备份，对于极端重要的繁忙数据处理工作业务，没有通过一定的备份方案来加强系统的安全性。

### 1.14 不重视对系统安全性方面的信息搜集和分析

制造企业信息集成平台的安全性是一个相对安全的过程，今天的安全不等于明天的安全，因为计算机系统中人们会不断发现新的各种各样的安全漏洞或隐患，而企业一般没有配备专门人员从各种渠道(包括因特网上的各类计算机安全网站、软件发行商、网络安全工程师或研究人员、有网络安全防范经验的人等等)搜集相关提高信息集成平台安全性方面的信息，对之进行相应修改或重新配置参数。另外对 WEB 日志、邮件服务日志、FTP 日志等信息的分析、对网络流量异常的预警、对系统网络性能的测试等方面没有进行认真分析过和处理过，而分析这些对网络安全有影响的数据可以加强安全防范措施，提出改进措施。

针对上述制造企业信息集成平台的安全性方面存在的问题，下面提出企业在信息化过程中应该采取的安全措施。

## 2 提高制造企业信息集成平台安全性的措施

随着企业信息化的深入发展，对制造企业信息集

成平台的依赖也越强，集成平台的安全问题必须做到防患于未然，一旦出现安全性问题，后果不堪设想。因此在企业集成平台的安全性方面，企业领导层必须重视起来。有必要建立一支计算机安全方面的小组，对信息集成平台进行详细的安全检查，制定计算机安全保障措施，及时处理网络中存在的不安定因素。下面从实用的角度提出提高制造企业信息集成平台的安全性措施。

### 2.1 引进或培养具有较高安全防范经验的高级人才

计算机安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。引进或培养具有较高安全防范经验的综合性高级人才，对于制造企业来说具有安全战略意义。这些人才要求具有扎实的网络知识功底、互联网知识，对信息安全、网络安全、软件编程、数据库知识精通，有较强的分析问题、解决问题的能力和协调能力，从而可从根本上保证企业信息集成平台的安全性的实施。

### 2.2 制定企业级详细的计算机安全管理措施和制度

俗话说“没有规矩，不成方圆”，详细制定企业级信息集成平台的安全管理措施可以减少计算机安全事故的发生。例如口令必须取6位字母数字以上；每个人的登录名和口令不能泄漏给第2个人，即由用户来管理自己的登录密码，系统管理员可以更改用户的密码，但不能读取用户的密码，用户必须对自己密码的安全性负责；当暂时离开计算机时，应进行屏幕口令保护；未经许可和检查不能用软盘拷入或拷出文件；各个部门未经许可不能自行购买或自带 Modem 拨号上网等。

### 2.3 统一规划企业网络　构造合理的 VLAN

为保证企业的网络安全，企业内部网中可将相同业务或业务紧密联系的各个部门或小组组成一个工作组，工作组与工作组之间，通过中心网络交换机在逻辑上用 VLAN（Virtual Local Area Network）隔离开来，每一个 VLAN 是一个独立的逻辑网络组，该组中的所有成员可以相互传输信息，不同组之间的信息传输通过交换机内部路由来实现。各个逻辑网络组之间可以通过设定 IP 地址过滤来拒绝某些计算机的跨网段访问。这样，当某个工作组 A 内部相互之间发送信息时，不需要向整个网络进行广播，既可以避免以太网中的数据包的冲撞，提高企业总体网络的传输性能，也保证了数据不会被工作组 A 以外的用户接收到；同时工作组与工作组之间没有经过 IP 过滤的用户可以相互访问，而经过 IP 过滤掉的用户无法进入另外的工作组。

此外对于比较重要的部门，可以根据实际情况再进行工作组内部 IP 地址的二次规划。可以将重要部门的局域网与企业内部网隔离开来，使得某些人只能在本部门访问而有些人却可以访问企业网；通过企业网只能看到本地服务器上的共享资源，而不能进入本地网的其它计算机，这样就可达到较好的安全防范效果。

### 2.4 尽量采用安全策略较高的操作系统

一般桌面操作系统不宜采用 Windows 95/98/Me，除非是单机系统，而应该采用 Windows NT Workstation 4.0/Windows 2000 、Linux 等作桌面操作系统。网络服务器采用版本较高的 Windows 2000 Advanced Server，Unix 系统、Linux 系统等等，注意对这些操作系统的补丁包的升级，可以经常查看软件发行商网站的补丁包。采用 Windows NT Workstation 4.0 或 Windows 2000 professional 桌面操作系统时，可以通过服务器 Windows NT Server 4.0 或 Windows 2000 Advanced Server 上的安全管理策略，禁止用户做出不利于安全的操作；在桌面端，通过参数设定，可以禁止普通用户进入“控制面板”中的“网络”，使得用户无法修改 IP 地址。仔细检查操作系统中的各项参数配置，确保操作系统的安全性。

### 2.5 统一分配访问权限　制定权限分配策略

企业内部网的权限控制可以提供针对企业内部网非法操作的安全保护。用户和用户组被赋予一定的权限。企业内部网控制着用户和用户组可以访问哪些目录、子目录和文件及其它资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。可以根据访问权限将用户分为几类，每一类规定其相应的权限，例如特殊用户（系统管理员）、域用户、备份用户、一般访客等。

### 2.6 购买必要的防火墙　隔离企业内部网和 Internet 连接

企业之间协作制造的信息传递应采用必要的安全措施。防火墙作为内部和外部网络之间的分水岭，在网络安全中扮演着举足轻重的作用。事实上，防火墙可以进行用户身份识别即验证用户身份、判断用户能否具有应该有的权限、数据完整性检验（检验数据在网络传递到达后是否被修改或丢失）、网络实时监控（动态掌握用户的活动轨迹）、监控网络数据流并发现危险所在并生成统计报表。对于以上策略都有相应的技术得以实现，诸如采用安全警卫、VLAN、网间的策略路由、加密和隧道技术、网络扫描数据包过滤等。网络防火墙确保了企业内部网的安全。目前可选用的网络防火墙较多，包括硬件防火墙和软件防火墙[6]。

对于企业之间协作制造的重要信息传递应采用必要的安全措施，包括采用 PPTP 协议（Point to Point Tunnel Protocol）的 VPN（Virtual Private Network）。在分布式的计算机网络环境下，VPN 的出现为企业之间相互访问提供了一种很好的解决方案。企业内部网之间可通过 Internet 及其它公用网相互连接起来，这样做比使用专用网更经济，同时，管理任务由 ISP 负责。可以相互登录到对方所在的企业网络中，实现信息互访，而数据在这个通道上传输是经过了加密处理的。

### 2.7 在研制应用软件系统时应制定周密的安全方案

在研制制造企业信息集成平台应用软件时，应充分考虑应用软件的安全性要求，制订周密的安全实施

方案,例如信息安全要求、数据库安全要求、访问控制安全等等,尽可能考虑操作留痕迹的日志管理功能,以便出现安全问题时,可以对出现的安全问题进行审计分析。在应用程序中,如果要确认信息的发送是由哪台计算机发出的,可以考虑用程序实现 IP 地址和网卡 MAC 地址的绑定来唯一确定进行了非法信息发送的计算机,这样可充分提高应用软件的安全性。

### 2.8 将各类文档存放到数据库中进行统一管理

在利用制造企业内部信息集成平台进行产品设计、开发、加工、制造、检验、包装、销售过程中,生成了大量文档,例如 Word 文档、PowerPoint 文档、WPS 文档、各类图片、图纸以及声音、动画、视频等等(统称为文档),可能这些文档分散存放于企业内部网的不同的目录下,如果不进行有效管理,可能会造成重要资料的失窃、信息泄漏等安全事故,要对这些信息进行查找也比较困难。可以考虑采用数据库对这些文档进行统一管理,从数据库一级保证其安全性,也大大方便了信息的查阅,实现快速查找。

### 2.9 其它方面应采取的安全措施

在服务器上安装网络病毒防火墙,例如 Kill 病毒防火墙,对于有病毒的邮件自动转回不予接受,这样也避免了诸如邮件炸弹等各种邮件病毒;对确实需要拨号上网的部门应单独配备一台计算机,同企业网络隔离开来。对于安全性特别高的场合,可用便携式验证器(如智能卡)验证用户的身份。通过相关工具经常性地分析和检查网络流量是否异常、分析 WEB 日志、邮件日志、FTP 日志等中的不安定因素,将对整个制造企业信息集成平台的安全预防起到很好的作用。

## 3 结束语

制造企业信息集成平台计算机安全是一项系统工程,需要一定的人力、财力和物力,必须引起企业领导在安全观念上的重视,同时将安全管理制度与安全管理技术结合起来,整个企业信息集成系统的安全性才有保证。

**参考文献:**

[1] 范玉顺,吴澄. CIMS 应用集成平台体系结构研究[J]. 计算技术与自动化,1996, 15(4): 39 - 44.
[2] 杨景宜. 机床制造业 CIMS 工程[M]. 北京:中国经济出版社, 1999.
[3] 胡家齐. 飞机制造企业 CIMS 工程[M]. 北京:中国经济出版社, 1999.
[4] 薛劲松,宋宏. CIMS 总体设计[M]. 北京:机械工业出版社,1997.
[5] 郑辉,涂奉生. 网络邻居共享存在的安全隐患分析[J]. 计算机工程,2001, 27(1):57 - 59.
[6] 刘渊译. 因特网防火墙技术[M]. 北京:机械工业出版社,1998.

# Security Condition and Countermeasures of the Information Integrated Platform in Manufacturing Enterprises

*WANG Cheng-liang*
(College of Software Engineering , Chongqing University, Chongqing 400044, China)

**Abstract**: Information integrated platform in manufacturing enterprises is a kind of software and hardware platform which supports application development, application integration and system running in complex information environment. The information processing of enterprises relys on this platform. Due to the increasing number of computer security problems, much attention must be paid to the security of information-integrated platform in manufacturing enterprises. The current security condition of information-integrated platform in manufacturing enterprises is introduced and the related countermeasures is also produced. In order to ensure the security, the conclusion that secure management system should be combined with secure management techniques is drawed .

**Key words**: manufacturing enterprises; information integrated platform; computer security

(编辑 吕赛英)