现代计算机技术与应用
2020 年 2 月第 2 卷第 1 期

How to ensure the information security of OA

Li Wenjing

Fujian Polytechnic of Information Technology, Fuzhou

Abstract: The construction of office automation system facilitates each unit to release information, share resources, communicate with the outside world and improve work efficiency, but it also brings various security threats from the outside network. In this paper, seven main preventive methods are put forward for common system security problems.

Key words: Office automation; Information security

Received: 2020-01-10; Accepted: 2020-01-25; Published: 2020-02-01

如何保障办公自动化的信息安全

李文静

福建信息职业技术学院，福州

邮箱：wjli54@126.com

文章引用：李文静. 如何保障办公自动化的信息安全 [J] 现代计算机技术与应用，2020，2（1）：9–14.

摘　要：办公自动化系统的建设方便了各单位发布信息、共享资源、对外交流和提高办事效率，但同时也带来了来自外部网络的各种安全威胁。本文针对性地对系统常见安全问题提出七类主要的防范方法。

关键词：办公自动化；信息安全

收稿日期：2020-01-10；录用日期：2020-01-25；发表日期：2020-02-01

办公自动化系统（OAS）是办公业务中采用 Intemet/Intranet 技术，基于工作流的概念，使企业内部人员方便快捷地共享信息，高效地协同工作，实现迅速、全方位的信息采集、信息处理，为企业的管理和决策提供科学依据。实现办公自动化的程度是衡量其现代化管理水平的标准。OAS 从最初的以大规模采用复印机等办公设备为标志的初级阶段，发展到今天的以运用网络和计算机为标志的阶段，OAS 对办公方式的改变和效率的提高起到了积极的促进作用。近年来，办公自动化系统都是架设在网络之上的，它是一个与外界联系的渠道，这种接入一方面方便了单位发布信息、共享资源、对外交流和提高办事效率，另一方面也带来了来自外部网络的各种安全威胁。

1　办公自动化系统存在的安全

随着 INTERNET 的迅速发展，如何保证信息和网络的自身安全性问题，尤其是在开放互联环境中进行商务等机密信息的交换时，如何保证信息存取中不被窃取篡改，已成为大家非常关注的问题。在国际上，计算机犯罪案件正在以

几何级数增长。计算机犯罪是一种高技术型犯罪，由于犯罪的隐蔽性，因此，对办公自动化系统安全构成了很大的威胁。

目前，办公自动化系统的安全隐患主要存在以下几个方面：

假冒内网的 IP 地址登录内网窃取信息；软件系统自身的问题：利用网络传输协议或操作系统的漏洞攻击网络；获得网络的超级管理员权限，窃取信息或破坏系统；在传输链路上截取信息，或者进入系统进行物理破坏；病毒破坏，计算机病毒是一种人为制造的，在计算机运行中对计算机信息或者系统起破坏作用的程序。它通常隐蔽在其它程序或者文件中，按照病毒设计者设定的条件引发，从而对系统或信息起到破坏作用；黑客入侵；防范技术落后，网络安全管理不力，管理人员混乱，权限混乱等等。

2　系统安全的防范

针对目前系统安全的上述问题，在办公自动化系统安全上提出下面几类主要的防范方法。

2.1　加强机房管理

对目前大多数办公自动化系统来说，存在的一个很大的不安全因素是网络管理员的权力太大，据有关资料报道，80% 的计算机犯罪来自内部，所以对机房工作人员要做好选择和日常考察，采取一定的手段来限制或者削弱网络管理员的权力，对机房工作人员，要结合机房、硬件、软件、数据和网络等各个方面的安全问题，进行安全教育，提高工作人员的保密观念和责任心；要加强业务、技术等方面的定期培训，提高管理人员的技术水平。

2.2　设置访问控制

访问控制是保证网络安全最重要的策略之一。访问控制策略包括人网访问控制策略、操作权限控制策略等几个方面的内容。首先，网络管理员应该对用户账户的使用、用户访问网络的时间和方式进行控制和限制。用户账户应只有网络管理员才能建立，用户口令是用户访问网络所必须提交的准人证。针对用

户登录时多次输入口令不正确的情况，系统应按照非法用户人入口令的次数给予给出报警信息，同时应该能够对允许用户给出进入信息。其次，用户名和口令通过验证之后，系统需要进一步对用户账户的默认权限进行检查。最后，针对用户和用户组赋予一定的操作权限。网络管理员能够通过设置，指定用户和用户组可以访问网络中的哪些资源，可以在服务器上进行何种类型的操作。网络管理员要根据访问权限将用户分为特殊用户、普通用户和审计用户等等。

2.3 数据加密

主要针对办公自动化系统中的数据进行加密。它是通过网络中的加密系统，把各种原始的数据信息（明文）按照某种特定的加密算法变换成与明文完全不同的数据信息（密文）的过程。目前常用的数据加密技术主要分为数据传输加密和数据存储加密。数据传输加密主要是对传输中的数据流进行加密，常用的有链路加密、节点加密和端到端加密三种方式。链路加密对用户来说比较容易实现，使用的密钥较少，而端到端加密比较灵活，对用户可见，在对链路加密中各节点安全状况不放心的情况下也可使用端到端加密方式。数据存储加密主要就是针对系统数据库中存储的数据本身进行加密，这样即使数据不幸泄露或者丢失，也难以被人破译。数据存储加密的关键是选择一个好的加密算法。

2.4 建立工作日志

对所有合法登录用户的操作情况进行跟踪记录；对非法用户，要求系统能够自动记录其登录次数，时间，IP 地址等信息，以便网络管理员能够根据日志信息监控系统使用状态，并针对恶意行为采取相应的措施。

2.5 加强邮件安全

在众多的通信工具中，电子邮件以其方便、快捷的特点已成了广大网络用户的首选。然而这也给网络安全带来了很大的隐患，目前垃圾邮件数量巨大、邮件病毒防不胜防，而关于邮件泄密的报道更是层出不穷。面对电子邮件存在的巨大安全隐患，可以采取如下的防御措施：

（1）加强防御，一般用户会经常忽略使用电邮安全的基本常识，因此教育用户一些常识是非常有必要的。例如，勿开启来自未知寄件者的附件；勿点选不熟悉来源的任何内容；封锁陌生人的实时讯息等。

（2）对邮件进行加密，由于越来越多的人通过电子邮件进行重要的商务活动和发送机密信息，因此，保证邮件的真实性和不被其他人截取和偷阅也变得日趋重要。据调查，74% 邮件泄密是因为邮件中的机密信息未做任何加密措施引起的。因此，邮件加密是一种比较有效的、针对邮件内容的安全防范措施，采取先进的加密算法可以有效地保障数据的安全。

（3）反垃圾邮件，垃圾邮件经常与病毒有关，因此用户需要反垃圾邮件和反病毒保护。垃圾邮件中的链接经常指向包含恶意软件的网站，而且病毒经常通过电子邮件传播。大大减轻邮件病毒肆虐的方法是使用反病毒软件，例如，只使用提供自动病毒保护功能的电子邮箱，只打开来源可信的电子邮件，或在打开邮件附件之前用反病毒软件进行扫描等等。

2.6 设置网络防火墙

通过安装并启用网络防火墙，可以有效地建立起计算机与外界不安全因素的第一道屏障，做到实时监控网路中的数据流，保护本地计算机不被病毒或者黑客和入侵。

2.7 保护传输线路安全

对于传输线路，应有相应的保护措施，并要求远离各种辐射源，以减少由于电磁干扰引起的数据错误；网络连接设备如 Hub 等应放置在易于监视的地方，以断绝外连的企图；还要定期检查线路的连接状况，以检测是否有外连或破坏等行为。

3 结语

总之，网络应用已经渗透到社会经济生活的方方面面，Internet 和信息化办公在为人民提供便利的同时，也时刻受到网络信息安全的影响。我们在充分享

受网络办公系统方便、快捷的同时，更要时刻注意维护系统信息的安全。

参考文献

［1］蔡奇玉．CGI 编程指南［M］．北京：机械工业出版社，1997.

［2］戚文静．网络安全与管理（第二版）［M］．北京：中国水利水电出版社，2008.