

企业电子商务中信息安全问题的研究

李凤慧

(潍坊学院, 潍坊 261061)

〔摘要〕 本文主要探讨了企业电子商务中信息所面临的主要威胁及电子商务对信息内容的基本要求。最后, 综合多种新技术, 提出了一些具体的、解决问题的对策。

〔关键词〕 电子商务; 信息安全; 对策

〔Abstract〕 The paper discusses main threats and requirements of information in enterprise's electronic commerce. Finally, integrating with many new technologies, it gives some useful and practical countermeasures.

〔Key words〕 electronic commerce; information security; countermeasures

〔中图分类号〕 F724.6 〔文献标识码〕 A 〔文章编号〕 1008-0821(2006)05-0190-02

1 引言

电子商务(Electronic Commerce)是网络经济时代兴起的一种崭新的企业经营方式,是企业基于 Internet 而进行的各种商务活动的总称。Internet 的开放性使电子商务具有了高效、快捷、方便等特点并迅速得到广泛应用,同时开放性也给电子商务带来许多威胁:病毒入侵、黑客攻击、电磁泄露,信息篡改、信息抵赖以及信息假冒等,给个人和企业带来了不可估量的损失。据报道,商业信息被窃取的事件以每月 260% 的速度在增加,这严重制约着电子商务的正常发展。电子商务的信息安全对企业来说是决定命运的关键,必须引起高度重视。

2 电子商务信息安全面临的威胁

2.1 人为或自然威胁

来自于各种自然灾害、恶劣场地环境、电磁辐射、电磁干扰、网络设备老化等自然威胁是不可预测的,会直接影响商务信息的安全;而人为威胁通过攻击系统的要害或弱点,破坏电子商务系统,如篡改、删除商务信息流的内容等,给企业造成不可估量的损失。

2.2 安全缺陷

电子商务以网络为平台,计算机系统的安全缺陷和通信链路的安全缺陷构成了商务网络信息系统的潜在安全缺陷。电磁辐射、电磁泄漏、搭线、串音等都会对信息保密构成威胁。因为攻击者可以通过接收装置,截获企业机密信息,或通过对信息的分析,获取账号、密码等有用信息,假冒用户消费、栽赃,假冒领导发布命令、调阅文件等。

2.3 软件漏洞

由于软件程序的复杂性和编程的多样性,在电子商务系统的软件中很容易有意或无意地留下一些安全漏洞。例如,陷门是程序模块未记入文档的秘密入口,一旦被原来的程序员利用或被他人发现,后果难以想象;而操作系统本身也存在许多安全漏洞如 I/O 非法访问、访问控制的混乱、不完全的中介、操作系统陷门等以及数据库的安全漏洞,都严重危及电子商务信息的安全;特别是 TCP/IP 通信协议,在设计初期没有考虑到安全性问题,因而连接到 Internet 的计算机系统就可能受到外界的恶意攻击和窃取;另

外,网络软件与网络服务、口令设置等方面都存在漏洞,对商务信息安全造成极大威胁。

2.4 病毒和黑客入侵

病毒是一种具有繁殖力、破坏力的程序,也会侵入电子商务系统而破坏数据和程序。在网络环境下,计算机病毒更具有不可估量的威胁性和破坏力;而黑客一般利用信息系统的漏洞或黑客程序来侵入系统,达到窃取别人的账号进行消费、获取对手商业机密、攻击对手商业网站等非法目的。

2.5 技术被动

在我国,电子商务信息安全还存在着技术被动而引起的安全缺陷。我国的芯片基本依赖进口,即使是自己开发的芯片也需要到国外加工,而且不少网络设备也是从国外引进的,这无疑是一种严重的安全隐患。因为它的维护和技术掌握在别国手里,假如软件中的可能漏洞被恶意利用,造成的后果将是不堪想象的。

3 电子商务对信息安全的要求

3.1 保密性

即防止信息泄漏给非授权用户,只为授权用户使用的特性。对用户的个人信息进行保密、维护商业机密是电子商务全面推广应用的重要保障。

3.2 完整性

完整性是电子商务信息未经授权不能进行改变的特性。商务信息在存储或传输过程中必须保持原样,不能被偶然或蓄意地删除、修改、伪造、乱序等。如果交易文件被篡改,将会失去交易的严肃性和公平性。

3.3 真实性

真实性是防止商务系统内的信息感染病毒或遭受恶意攻击,以确保信息的真实可靠,不能存在欺诈行为。

3.4 可靠性

可靠性是指商务信息系统能够在规定条件下和规定时间内完成规定功能,是电子商务系统安全的最基本要求之一,也是所有网络信息系统的建设和运行目标。

3.5 可用性

指电子商务信息可被授权实体访问并按需求使用,通

收稿日期:2006-01-14

作者简介:李凤慧(1970—),女,毕业于山东科技大学,硕士,潍坊学院公共计算机教学部讲师,研究方向:企业信息管理、电子商务。



过身份识别和访问控制等手段,允许授权用户使用相应权限的资源,防止和限制非法访问。

3.6 不可抵赖性

即不可否认性,指电子商务信息在交互过程中,确信参与者的真实同一。参与者不能否认曾经完成的操作,交易一旦达成是不能抵赖的,否则将损害对方的利益。

3.7 可控性

可控性是指对电子商务信息的传播及内容要有控制能力。

4 电子商务信息安全对策

4.1 反病毒技术(Antivirus)

计算机病毒的防范是电子商务信息安全建设中重要的一环。病毒的处理本着“预防为主、治疗为辅”的原则。积极采取多种措施进行预防:如对新购置的计算机硬件、软件进行病毒检测;经常进行数据备份;用硬盘启动服务器;对网络目录和文件设置访问权限;对服务器中文件进行实时扫描和监测;系统管理员的口令应严格管理,且经常更换,保证网络系统不被非法存取;在工作站上采用防病毒芯片;在服务器上安装防病毒系统;当出现病毒传染迹象时,应立即进行隔离等等。

一旦确定计算机系统感染了病毒,应该立即清除、恢复系统。病毒清除要本着以下原则:用干净盘引导系统,在无毒的环境中清除病毒;启动盘和杀毒盘加上写保护;尽可能找出病毒的宿主程序;清除工作要深入全面,保证清除工作的正确性,修改了的文件转换过来;不能用病毒标识免疫方法清除病毒;对于混合型病毒清除要彻底;对文件型病毒检查系统中其他类文件是否也被感染等等。

4.2 防火墙技术(Firewall)

防火墙技术就是近年来提出并推广的一项网络安全技术,是目前一种最重要的网络防护设备。防火墙位于两个(或多个)网络间,是实施网络之间访问控制的一组组件的集合,是一个把互联网与企业内部网隔开的屏障。它的目的就是在网络连接之间建立一个安全控制点,通过允许、拒绝或重新定向经过防火墙的数据流,实现对进、出内部网的服务和访问的审计和控制,从而保护企业内部网免受非法用户的侵入,保护内部网络的设备不被破坏,防止内部网络的敏感数据被窃取,增强企业内部网的安全性。防火墙常用技术如下:

数据包过滤技术是在网络层中对数据包实施有选择的通过,依据系统内事先设定的过滤逻辑,检查数据流中每个数据包,根据数据包的源地址、目的地址、所用的TCP/UDP端口与TCP链路状态等因素来确定是否允许通过;应用网关技术是建立在网络应用层上的协议过滤,它针对特别的网络应用服务协议即数据过滤协议,能够对数据包分析并形成相关报告。应用网关对某些易于登录和控制所有输入输出的通讯环境给予严格的控制,以防企业敏感程序和数据被窃取;代理服务技术利用代理服务器来限制或者完全拒绝网络上基于SMB的连接。代理服务程序在客户程序和真正的服务器程序之间起到一个中间节点的作用。

4.3 数据加密技术(Data encrypt)

数据加密是指采用某种算法把原始数据进行再组织,然后在网络的公共信道上进行传输,非法接收者因没有密钥,无法得到原始数据,而合法的接收者可以根据密钥进行解密,得到原始数据。加密技术可实现数据的保密,但非法接收者可能通过泄漏、窃取或破译等方法获取正确密

钥。为了降低被破译的危险,需要建立严密的密钥管理机制,提高工作人员的素质,加长密钥数位长度。密钥数位越长,越安全,但加密和解密的时间也越长,数据传输效率越低。所以,要根据电子商务对安全要求的不同级别来选择密钥的长度。

目前加密体制分为两大类:私钥(单钥或对称)加密体制和公钥(双钥或非对称)加密体制。由于公钥加密体制是一种双密钥加密体制,所以接收方对加密的数据不能进行篡改或伪造,这样就保证了数据的保密性、完整性和不可否认性等。目前最著名的公钥加密体制是RSA体制,它是由美国科学家提出的、目前应用最广泛的公钥加密算法。尽管目前加密算法很多,加密技术也很强,但往往不尽人意。因为,不同的厂商可能采用不同的标准,从而带来了兼容性问题,这严重阻碍了商务交易活动在安全基础上的高效性。人们需要的是一个确实贯彻了加密体制的、针对企业环境开发的、通用的加密系统。

4.4 虚拟私有网技术(VPN)

虚拟私有网是使用开放的公共信道,通过附加的协议处理,向用户提供的虚拟私有网络。VPN的实现过程使用了安全隧道技术(STT)、信息加密技术、用户认证技术、访问控制技术。STT使用加密与封装相结合的技术对用户数据进行安全保护,是实现VPN的核心技术。STT对用户应用数据进行加密处理后,封装到网络传输协议的PDU中,然后通过外部协议的传输机制将内部的应用数据传递到对等实体,经过解封装处理后提交上层应用。

4.5 授权认证(CA)

国际通行的解决电子商务安全问题的做法是采用CA安全认证系统。CA认证中心并不是安全机构,而是一个受大家信任的第三方机构,是电子商务中的仲裁机构。在电子商务系统中,所有实体的数字证书都是由CA证书授权中心分发并签名的。一个完整、安全的电子商务系统必须建立起一套完整合理的CA体系。

在电子商务的各个环节,交易的各方都需验证对方证书的有效性,从而解决相互信任问题。CA体系借助数字签名、身份识别等技术手段,解决网络身份的认证以保证交易各方身份是真实的;解决数据传输的安全性以保证在网络中流动的数据没有受到破坏或篡改;解决交易的不可抵赖性以保证对方说的话是真实的。

4.6 自主的信息技术产品

自主的信息产业或信息产品国产化是信息安全的根本。必须加强基于自主技术的信息安全技术与产品的开发与应用,建立起独立自主的信息安全产业。国家要制定相关政策,加大对自主知识产权产品在资金、技术、人力等方面的投入,加强关键核心技术的科研攻关和创新,大力发展自主的专用芯片、自主嵌入式操作系统和自主的密码技术产品等,以确保商务信息系统的安全。

当然,保障电子商务的信息安全,除了开发有效的网络安全技术外,同样离不开完备的安全政策法规和有效的物理安全机制,只有这样,才能保证电子商务的健康持续发展。

参考文献

- [1] 魏琦, 张明光. 电子商务的安全对策[J]. 江苏商论, 2005, (1).
- [2] 刘法胜. 大学IT[M]. 东营: 石油大学出版社, 2004. 7.