维普资讯 http://www.cqvip.com

企业信息安全问题及解决方案

林 山

(重庆大学计算机学院 重庆 400030)

摘 要 企业信息安全是目前我国企业普遍面临的问题,本文分析了当前企业安全问题的现状以及相应的对策,希望对企业的信息安全提供一些有价值的借鉴和参考。

关键词 企业信息,安全策略,解决方案

1 引言

随着信息技术的广泛应用,电子商务为企业的经济发展提供了一个崭新的舞台,它把信息网络、金融网络、物流网络和经济网络等多种网络信息紧密地结合在一起;它把人们的商务活动和贸易活动的方方面面通过网络连接在一起;它使得信息流、资金流和货物流能够高效快捷地流动起来。

但是,电子商务在我国并没有得到普及和深入。一个重要的原因就是电子商务的安全性,任何企业和商业机构都不会通过一个不安全的网络进行商务交易。另外,一些不法分子也会千方百计偷取企业的机密,给企业造成巨大损失。所以,企业的信息安全问题也越来越成为人们关注的焦点。

2 企业信息安全存在的隐患

(1)信息的截获和窃取 如果没有采用加密措施或加密强度不够,那么攻击者就可能通过互联网获取企业的银行帐号、密码以及企业的事业机密。

(2)信息的篡改 攻击者可以通过篡改、删除或插入的方法,改变企业收发的信息。

(3)信息假冒 攻击者可能通过伪造电子邮件或假冒他人身份发送信息来欺骗用户。

(4)交易抵赖 交易的一方事后否认交易的存在,从而给另一方造成经济损失。

(5)信息损毁 由于人为或非人为的原因,造成信息被删除或破坏。

目前,我国很多企业都缺乏网络安全意识,包括众多的政府网站、商务网站都没有采取必要的防范措施,这样的薄弱实在令人不寒而栗。此外,多年来IT技术与产品研发能力的相对滞后,造成大量核心技术与产品都是舶来的洋货,而在引进时根本没有能力进行必要的安全检测。因此,如何应对Internet普及而带来的日益增长的信息安全问题,是企业必须解决的急迫问题。

3 信息安全策略

网络信息安全需要从技术和管理两方面入手。因此,网络安全策略分为技术策略和管理策略。

(1) 技术策略

·安装使用网络安全检测设备和相关软件借助一些专用的网络安全监控设备和软件,加强对各种不法行为的监控和防范。

·加强网络访问控制是网络安全防范和保护的主要策略。它包括入网访问控制、网络权限控制、网络监测和锁定控制等。

·安装网络杀毒软件,保护企业网络所有的可能病毒入口不受病毒的侵袭。

·采用防火墙技术防火,墙用来检查通过内部网和外部网间的信息往来,它可以鉴别网络服务请求是否合法,以便采取响应或拒绝的措施。

·数据加密是采用一定的加密技术,以防在传输过程中数据一旦被截获不致造成信息的泄露,其核心是加密的方式以及密钥的分配和管理。

·引入鉴别机制,鉴别是查明另外一个实体身份和特权的过程,以确定其合法性,并作出响应。

·安全协议的建立和完善是安全保密系统走上规范化和标准化的基本因素。安全套接层ssL(secure sockets Layer)协议是目前Internet上使用最广泛的安全协议,该协议向TCP/IP的客户/服务器型提供了客户端和服务器的身份认证、会话密钥交换和信息链路加密等安全功能,确保网络传输的数据包不会被第三者监听和篡改。

·入侵检测系统可以帮助系统对付网络的攻击,扩展了系统管理员的安全管理能力,提高了信息安全基础结构的完整性。

(2)信息安全管理策略

·加强电子商务网络系统的日常管理和维护;

·建立严格的保密制度;

·加强对管理人员监督和培训,落实工作责任制;

维普资讯 http://www.cqvip.com

- 建立跟踪、审计和稽核制度；
- 完善病毒防范制度；
- 建立健全相关法律法规制度；
- 多人负责，任期有限，职责分离。

4 企业信息安全的解决方案

企业网络的安全体系涉及到网络物理安全和系统安全的各个层面。应从以下三个方面进行综合考虑。

4.1 安全体系

按照安全策略的要求及风险分析的结果，整个企业网络的安全措施应根据不同的行业特点，按照网络安全的整体构想来建立。

4.2 物理安全

保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提。物理安全是保护计算机网络设备、设施以及其他媒体免遭地震、火灾和水灾等环境事故以及人为操作失误或各种计算机犯罪行为而导致的破坏过程。主要包括环境安全、设备安全、媒体安全三个方面。

4.3 系统安全

网络的各个层面都可能对系统安全构成威胁。网络的七层在不同程度上会遭受到不同的攻击。通常，系统安全主要关注网络系统、操作系统和应用系统三个层次。

(1) 网络系统

网络系统的安全是由网络的开放性、无边界性和自由性造成的，安全解决的关键是把被保护的网络从开放、无边界性和自由的环境中独立出来，使网络成为可控制、可管理的内部系统。解决网络安全的主要方式有：

网络冗余——解决网络单点故障的重要措施。对关键性的网络线路和设备通常采用双备份或多备份的方式，以保证网络正常地运行。

系统隔离——分为物理隔离和逻辑隔离。主要是从网络安全等级来考虑划分合理的网络安全边界，使不同的网络或信息媒介不能相互访问，从而达到安全的目的。

访问控制——对于网络不同信任域实现双向控制或有限访问的原则，使受控的子网或主机访问权限和信息流向能得到有效的控制。

身份鉴别——是对网络访问者权限的识别。一般通过三种方式验证主体的身份：一是主体了解的秘密，如用户名、口令等；二是主体携带的物品，如磁卡、IC 卡等；三是主体特征或能力，如指纹、声音等。

加密——目前加密可以考虑在三个层次上实现，即链路层加密、网络层加密和应用层加密。通过网络加密可以构造企业内部的虚拟专网(VPN)，使企业在较少的投资下得到安全较大的回报。

安全检测——采取信息侦听的方式寻找未授权的网络访问尝试和违规行为，包括网络系统的扫描、预警、阻断、记录和跟踪等，从而发现系统遭受的攻击伤害。

网络扫描——网络扫描系统能够对检测到的漏洞信息形成详细的报告，包括位置、详细描述和建议的改进方案，使网管能检测和管理安全风险信息。

(2) 操作系统

操作系统是管理计算机资源的核心系统，它负责信息的发送、管理设备存储空间和各种系统资源的调度。操作系统安全分为应用安全和安全漏洞扫描。

应用安全——面向应用选择可靠的操作系统并按正确的操作流程使用计算机系统，杜绝使用来历不明的软件，安装操作系统保护与恢复软件并做响应的备份。

系统扫描——基于主机的安全评估系统是在严格的基础上对系统的安全风险级别进行划分，并提供完整的安全漏洞检查列表。

(3) 应用系统

企业应用系统大体分为办公系统、业务管理系统和业务服务系统。企业应用系统的安全除采用通用的安全手段外主要将根据自身经营及管理的需求来进行开发。

办公系统——主要包括文件(邮件)的安全存储和安全传送。

业务系统——主要面向业务管理和信息服务的安全需求。

结束语 企业网络安全只是一个暂时的安全，随着时间的推移，各种内外因素的变化，该安全系统的安全性也将会发生变化。因此，网络安全是相对的，是相对人、系统、应用和时间而言的。要动态地调整信息安全规划，根据世界网络安全的形势变化，不断提升本企业的信息安全状况，在保护自己信息安全的同时，追求更大的经济利益。

参 考 文 献

1 周学广，刘艺. 信息安全学. 机械工业出版社
2 陈鸣，等译. 计算机网络. 机械工业出版社
3 谢希仁. 计算机网络. 电子工业出版社