内网安全技术浅析

张哲宇[1] 林逸祥[2]
（1.厦门大学 信息科学与技术学院；2.厦门大学 软件学院 福建 厦门 361005）

[摘 要]对当前内网安全技术进行阐述，并介绍应对内网安全的几个策略．主要有网络准入控制及防水墙技术。通过大量的调研和资料收集工作，全面地阐述内网安全技术的背景及其含义，针对当前内网安全技术的主要问题分析其相关处理方法，综述内网安全相关技术及其策略，并通过对内网安全的相关分析，探讨内网安全技术的未来方向及其未来可能发展的趋势和技术。

[关键词]内网安全技术 策略 网络准入控制 防水墙
中图分类号：TP3 文献标识码：A 文章编号：1671－7597（2009）1120071－02

一、内网安全技术的提出

近年来，内网安全事件频频发生。这些内网安全事件对政府、企业造成的损失和影响是十分巨大的。为了防止企业或组织内部重要或敏感数据的丢失，很多用户购买了昂贵的网络防护设备，甚至安装了多套防病毒软件，但是关键信息泄露问题还是没有得到很好的解决。造成以上问题的主要原因是，以往人们只重视外网对内网的威胁，而忽视了内部网络的自身的问题。相比之下，内部人员更容易通过网络或移动存储设备把敏感的信息泄露出去，人为原因造成的损失往往是不可估计，对企业或组织的破坏是十分巨大的。针对这一不可忽视的问题，国内外厂商纷纷提出了自己的内网安全标准，内网信息安全越来越多受到关注。

二、内网安全威胁

（一）严重的信息外泄

随着先进的网络及应用技术的发展，数据和设备的共享性得到了很大的提高。这给企业的管理和工作带来效率的同时，也产生了严重的信息外泄问题。而据统计，大部份机密、敏感数据都是被内部员工通过合法或非法手段，在企业内部网络系统的桌面终端计算机上通过各种传输、复制途径泄露出去的。

（二）病毒、蠕虫的入侵

目前，对病毒、蠕虫的入侵防范仍停留在网络边缘阶段。大部分企业开始在网络边缘部署放病毒软件，防火墙，防病毒网关，IDS等安全设备，但是这几种设备均是基于对已知攻击手段的防范，无法有效防范未知攻击手段。其实病毒、蠕虫的入侵威胁主要来自于内部网络用户的各种危险应用。

三、内网安全防范措施

（一）安全意识是根源

长期的安全攻击事件分析证明，很多攻击事件是由于人员的安全意识薄弱，无意中触发了黑客设下的机关、打开了带有恶意攻击企图的邮件或网页造成的。针对这种情况，首要解决的问题是提高网络使用人员的安全意识，定期进行相关的网络安全知识的培训，全面提高网络使用人员的安全意识，是提高内网安全性的有效手段。

（二）策略是关键

内部安全策略是一种指导方法，通常都以一种规范、制度、流程等体现出来，用以指导我们快速、合理、全面的建设内部安全系统，同时我们所规划和实现的内部安全策略本身又是可扩展的，随着时间的不断推移和内部安全需求的进一步变化，可以根据调整单位的内部安全策略来更好的指导内部安全系统的建设。

（三）技术是保障

技术是管理的一个辅助工具。一个工具怎么用，能不能用好，最终的落脚点还是要看管理。不同的企业用同样的产品，产生的结果是不一样的。当然，有了有效的管理策略，没有技术的保障实施，一切也都是纸上谈兵。总之，只有拥有一批高素质的网络使用人员，优秀的管理，再加上技术的辅助，才能保证内网的安全。

四、内网安全相关技术

（一）网络准入控制技术介绍

1．网络准入控制定义

思科网络准入控制（Network Access control，NAC）是一项由思科发起、多家厂商参加的计划，其宗旨是防止病毒和蠕虫等新兴黑客技术对企业安全造成危害，最早于2003年11月提出。借助NAC，客户可以只允许合法的、值得信任的端点设备（例如PC、服务器、PDA）接入网络，而不允许其它设备接入。 几个行业分析机构对网络接入控制（NAC）技术进行了思考，每家都使用了不同的术语集和差异很小的网络准入控制定义。例如，Forrester使用“网络隔离（Network Quarantine）”，而Meta用“端点访问控制（Endpoint Access Control）”。

2．网络准入控制的设计理念

撇开复杂的商业利益争夺，各厂商推出的网络准入控制技术虽然称呼各有差异，但核心设计理念是基本相同的，具体来讲，就是在网络节点接入安全网络时，需要对待接入的系统安全状况以及操作该节点系统用户的身份进行充分的评估、认证，以确定该系统是否符合网络的内部安全策略，来决定该网络节点系统是否接入到安全网络中，还是拒绝接入或安全升级后接入。显然，网络准入的机制不仅实现了安全网络“主动”的动态扩展，而且能够有效降低不可信终端系统接入网络所带来的潜在安全风险。

3．网络准入控制技术的特点

（1）可评估使用所有访问方法，包括LAN、无线、远程访问和WAN的所有终端，来进行全面控制；（2）终端可视性和控制确保可管理的、不可管理的、访客和恶意设备均符合企业安全策略；（3）终端控制的全程支持可自动执行终端的评估、验证、授权和修补流程；（4）将集中策略管理、智能网络设备及网络服务与多家著名防病毒、安全和管理供应商提供的解决方案结合在一起，以提供精确的准入控制管理；（5）基于标准的、灵活的API允许多个第三方参与整体解决方案，从而支持丰富的合作伙伴和技术生态系统。

4．网络准入控制技术所控制和解决的问题

（1）控制哪些人能接入LAN并限制他们能够访问的资源；（2）限制不值得信赖或者未知的用户，例如承包商、技术人员、远程用户或者离线员工等；（3）限制能够访问重要财务记录或者客户记录的人员；（4）根据职责、时间、地点以及应用程序来控制对数据的访问；（5）将用户分级以符合规定要求；（6）保护系统免受已知或者未知恶意软件的攻击；（7）简化事件反应；（8）保护关键应用服务（如VoIP）。

（二）防水墙技术

1．防水墙定义。“防水墙”（WaterWall）是相对于“防火墙”（FireWall）的一个概念，它是用来加强信息系统内部安全的重要工具，主要为防止内部信息向外扩散。具体说来，防水墙技术是一个以内网安全理论为基础，以数据安全为核心，利用密码学技术、PKI技术、操作系统核心技术、访问控制技术、审计跟踪技术等技术手段，对涉密信息、重要业务数据和技术专利等敏感信息的存储、传播和处理过程实施安全限制保护，最大限度地防止敏感信息外泄的内网数据保护技术。

2．防水墙系统设计理念。防水墙系统的设计理念是保护用户敏感信息不被非法外传、防止泄密事件发生，从而保证内部安全。它主要从以下五个方面来保障内网安全：

（1）失泄密防护；（2）文件安全服务；（3）运行状况的检测；（4）系统资源管理；（5）扩展身份认证。

在五个方面的大前提下，开发系统成为当代防水墙系统技术研究开发的主流设计理念。

（三）防水墙技术分析

防水墙作为加强信息系统内部安全的重要工具，它处于内部网络中，是一个内网监控系统，其着重点是用技术手段强化内部信息的安全管理，利用密码、访问控制和审计跟踪等技术手段对公司信息实施安全保护，使之不被非法或违规的窥探、外传、破坏、拷贝、删除，从本质上阻止了机密信息泄漏事件的发生。

（四）防水墙系统的特点

1．管理桌面计算机系统的规模大、效率高、策略周全，将单位全部的个人桌面系统纳入管理范畴，解决了桌面系统的安全问题。

2．针对网络通信、外设接口等可能成为失泄密途径，以周全的内部系统信息泄露保护体系，结合网络内部现有的其它安全系统，可构成强大、完备的内部系统信息泄露保护体系。

3．处理计算机的硬件配置和软件安装的系统资源，动态获取、更新和审计。杜绝了未经批准就安装和运行任何一款硬件设备和软件系统。

4．对全部个人计算机系统集中在防水墙的管理之下，集中管理安全策略、系统配置、安全事件和安全事故。

（五）防水墙系统在网络中的位置

管理员通过管理工作站来管理防水墙服务器，定制与实施相关的安全策略，防水墙服务器通过位于各部门的客户端工作站点来实现对整个内部网络的“用户身份”、“数据安全”、“设备安全”和“综合安全审计”等方面的综合管理和安全监控。

（六）防水墙控制和解决的问题

1．身份验证机制；2．访问控制体系；3．“非法外联”控制；4．设备密级标识；5．动存储介质的有效管理；6．安全审计；7．非法主机控制。

五、内网安全技术发展方向

（一）内网安全重心继续向终端计算机转移

传统的内网安全主要是注重服务器区域的安全管理，而随着终端机数量的增多，安全隐患也就越来越大，任何一台出现安全隐患，对整个内网都可能会产生巨大的冲击和破坏。因此，内网安全管理开始从服务器区域转向了终端计算机。

（二）终端安全产品向功能高度集成发展

随着技术的发展，企业用户逐渐认识到，内网的安全管理是一个有机的整体，不是靠几种安全产品的简单堆砌就能解决的，采用高度功能集成的安全产品可能是一个更好的选择。所以，未来的安全产品将朝着高度功能集成的方向发展。

（三）终端安全加固与运行维护并重

终端计算机作为内网的一部分，而且是员工日常工作的工具，当然要保证其安全性。不过，企业用户逐渐认识到，终端计算机的使用最终目的是为了降低成本、提高效率。因此内网既要有较高的安全性，也要能够易于维护。应该通过技术手段提高终端计算机的维护管理水平。所以，在内网安全管理方面的技术发展是提高内网安全管理的有效途径。

六、结论

随着社会的信息化以及网络的飞速发展，企业的内网规模和复杂度迅速提升，企业、国家对内网安全的需求不断增长，内网安全管理的技术和策略尤为重要。根据公安部发表08年《全国信息网络安全状况调查报告》调查显示，攻击或病毒传播源来自内部人员的比例同比增加了21%；涉及外部人员的同比减少了18%，说明联网单位对外部网络攻击防范的意识有所增强，但单位内部的网络安全管理工作还不到位。网络（系统）管理员通过技术监测主动发现网络安全事件的占66.28%，同比增加了13%，说明网络（系统）管理员安全技术水平有所提高；而通过安全产品发现的比例同比减少了8%，原因是目前计算机病毒、木马等绕过安全产品的发现、查杀甚至破坏安全产品的能力增强了。所以，安全技术的提升固然重要，管理人员的素质的提升和安全管理的策略更为重要。安全技术和安全管理不可分割，它们必须同步推进。因为即便有了好的安全设备和系统，如果没有好的安全管理方法并贯彻实施，那么安全也是空谈。

参考文献：

[1]丁谊，内网安全初探[J].科技信息，2004.2.

[2]介斐，企业内网安全防护解决方案[J].石油化工建设，2007.4

[3]赛迪网，内网安全技术分析与标准探讨.

[4]应对企业内网安全挑战的常见策略.

[5]浅谈内网安全的新宠儿——防水墙，ISSN:1009-3044.0.2006-14-051.

作者简介：

张哲宇（1988-），男，汉族，福建厦门人，厦门大学信息科学与技术学院通信工程系06级本科生；林逸祥（1988-），男，汉族，广东湛江人，厦门大学软件学院软件工程系06级本科生。

（上接第37页）

为可行的方式为分级授权，可以为不同的用户开放不同权限，比如校管理层拥有网络全部访问权限。一般的教师拥有一定权限，这部分可以精确到个人，也就是实行实名精确到个人的授权，对于普通学生开放受限的GUEST帐户，分级管理保障信息的安全。

同时，我们对不同的信息进行分类管理：对机密信息严格规定只能用于不联网的计算机，决不上网；专用内部信息使用专网连接，与校网分离，有的还设置加密传递；校内公开信息限校内访问，与Internet公众网间设置防火墙隔离。开展定期检查，以提高安全意识。

（三）网络数据备份与恢复

数据是整个校园网信息安全的核心。设备可以替换，但数据被破坏或丢失，其损失无法计量。所以设计一套完整的数据备份和恢复系统是校园网迫切需要的。它要考虑多方面因素，如备份／恢复数据量大小、应用数据中心和备援数据中心之间的距离及数据传输方式、灾难发生时所要求的恢复速度、备援中心的管理及投入资金等。

四、小结

综上所述，现有网络信息安全技术包括防火墙技术、入侵检测技术、访问控制技术、网络安全漏洞扫描技术、网络防病毒技术、信息加密技术、信息确认技术等，校园网络信息安全措施可通过综合以防火墙技术、入侵检测技术等为代表的硬件级措施和以病毒防御、身份确认等为代表的软件级措施来实现。在学校的校园网上实践的以防火墙技术为核心的硬件级保护和以防病毒技术为核心的软件级保护相结合的校园网络信息安全防护体系证明了这一点。

参考文献：

[1]MichaelE.whitman等著，齐立博译，信息安全原理（第二版），清华大学出版社，2006，3(1).

[2]冯登国，国内外信息安全现状及发展趋势（摘编），信息网络安全，2007（1）：9-11.

[3]熊心志，计算机网络信息安全初探，计算机科学，2006，55（B12）：60-62.

[4]李俊婷等，计算机网络信息安全及其防护措施，计算机与网络，2007（15）：45-46.

[5]邓志宏等，基于PKI的网络信息安全模型的研究与设计，计算机工程与设计，2007，28（2）：549-550，594.

[6]段友祥等，基于cA技术的网络信息安全系统设计实践，计算机工程与设计，2006，27（6）：1014-101.

[7]沈吉锋等，校园网安全防范策略，中国科教创新导刊，2009，2：165.