浅谈地级市电子政务外网安全审计

文／高爱乃·太原理工大学轻纺美院

本文就地级市电子政务外网安全审计系统进行了论述。电子政务外网的安全管理很重要，它直接影响政务网络的安全运行。政务外网中的安全问题其实大部分都是由客户端引起的，因此一定要在运行的前期就部署和设计客户端的审计和控制。如果忽视客户端的审计和控制，那么就会完全失去客户端的安全功能，就会给后期的网络运行带来极大的隐患和麻烦。

一、引言

安全是电子政务的重要环节。从各省市的政务外网建设情况来看，政务外网都大量采用了符合自己的安全设备和安全软件重点防范外部入侵，如防火墙、网关过滤、入侵监测、防病毒、邮件过滤、网页防篡改、物理隔离设备等；对于内部网络中违规、越权操作的管理，防范考虑则较少。

据CompTI（计算机技术行业协会）发布的安全调查报告显示：在网络安全事故中，约63%的事故是因人为因素所造成的；只有8%的网络安全事故是因技术原因所引起的。越来越多的专家和用户认为，约有70%的网络安全事故来自于网络内部。Gartner调查显示：超过84%的安全事件是内部人员把机密资料泄漏到外面的。Gartner Research分析显示：USB闪盘、MP3播放器以及当前类似的产品让用户在工作环境自由使用的同时，就可能突破网络的安全防线，导致数据泄漏。内部信息安全已经成为电子政务的安全威胁当中最为严重的问题，内网中安全隐患有：敏感文件被非法传阅、重要文件被非法修改或删除、重要的文件被非法拷贝外带、随意更改IP造成网络冲突、有意或无意攻击其它内部机器、数据库被有意或无意的破坏等。

安全审计系统可实现全网的数据安全防护体系，它控制用户计算机的外围设备和存储媒体的连接、使用和通信。它可以控制对物理埠（USB，FireWire，PCMCIA，串口，并口）、无线埠（蓝牙，WiFi，红外）和存储媒体(CD/DVD drives，Flash drives，Zip drives，Floppy drives，Tape drives)的访问。管理员可以制定访问权限控制策略，从而极为灵活地为不同类型用户设置不同权限。周密的防御措施与反篡改技术使得政务外网无法被攻破。

二、地级市电子政务外网安全审计基本原则

地级市电子政务外网安全审计的基本原则是在非常有效的信息安全控制和新科技的收益中达到最佳平衡，使政务网的珍贵电子数据得到最有效的防泄露控制。其实现主要通过以下措施：

（1）从内核深层次的防护。终端安全措施不只在设备本身的识别上，与其所运行的操作系统有关。解决这一点最有效的方法是在内核驱动层面上进行设计，在信息到达操作系统前进行分析。

（2）快速简便地对终端安全策略进行设计和修改。管理员能够通过政务的需要迅速地实现网络的安全控制。对于权限设置应基于“积极防护”的原则，即所有设备在没有管理员授权的情况下，应当被锁住。

（3）保证用户或黑客不能篡改、控制。黑客以及想使用未被授权设备的内部员工，可能尝试越权访问。防护措施应当具有冗余的、多层次的防篡改特性，使终端用户无法入侵或篡改权限。

（4）交互性和可操作性。管理员应当实时了解系统的薄弱环节，并制定策略防范可能的威胁。有效的端点防护措施可以分析终端节点的状况并发现潜在的危险。显然，政府里的不同人员应该享有不同的访问权限。举例来说，管理者通常需要为高级管理人员分配比普通公务员更高的权利。

（5）确保系统的安全策略控制了所有设备的使用。随着通信和存储协议（如USB，蓝牙，IrDA，WiFi）数量的日益增多，保证终端安全措施控制所有设备是至关重要的。此类产品必须在多种操作系统环境下，最大程度地对各种可能会使用到的设备进行测试。

（6）与现有的网络管理相结合。管理员通常要求：新的安全解决方案可被快速地部署到他们现存的网络结构中，并且可以方便地对网络的所有终端节点进行配置。

（7）活动记录与严重异常警告。管理员需要保存终端节点活动的详细日志，以便分析终端节点的防护效果。有效的防护措施可以与现有的预警管理软件无缝集成，以便协同工作。

（8）对用户的干扰最小。所采取的措施要在保证所有策略机制正常运行的条件下，对用户的干扰应减至最小，只有在出现异常时，才弹出连接监控程序；同时，对终端用户的手提电脑或台式机的影响必须减至最小。

（9）避免造成网络或个人主机负担过重。有效的措施应当在不对网络或个人终端节点的运行、存储资源产生过大负担的情况下，保证安全策略的实施。

三、地级市电子政务外网安全审计系统的主要功能

地级市电子政务外网安全审计系统应有以下的主要功能：

（1）接口控制。全面监控所有网络用户终端，控制所有外围设备和台式机及笔记本电脑，包括：物理接口（USB，FireWire，PCMCIA，串口，并口）、无线接口（WiFi，蓝牙，红外）、可移动媒介（可移动内存、光驱、软驱、SD卡、闪存、ZIP驱动器，磁带驱动器），以及提供全面的保护，以防止政务网数据终端的数据泄露。

（2）设备控制。可识别产品类型、型号和序列号，自动对USB，FireWire和PCMCIA按照类型、型号和唯一的序列号进行分类。管理者可以依据这些细节制定策略。比如，阻止所有USB设备，但仅允许USB打印机使用。

（3）存储控制。安全审计系统可以很方便地管理存储媒体。安全审计系统可以打开或关闭对CD/DVD、Floppy、Flash、Zip以及Tape驱动器的访问，还可将任意连接到这些端口的存储设备的操作模式设置为“只读”状态，使得文件可以被访问，但是新的信息不能被写入到这些媒体上。此外，安全审计系统可以对存储媒体设置最大的存储容量，例如128MB。在员工们享受廉价可移动的存储设备给生产力所带来优势的同时，管理员也可以保证用户不会利用这些先进的技术把大量的地级市政务外网信息带出地级政务外网。

（4）安全措施。阻止所有未验证的端口和设备的访问。安全审计系统对于新出现的产品，也可以得到保护。当出现新产品，管理者不用频繁升级冗长的设备阻止列表。

（5）多协议实时分析。对进出数据进行多协议实时分析，对于所连接的设备使用内核级验证，避免可能的疏漏，比如通过对操作系统伪造设备身份。

（6）防篡改技术。使用先进的防篡改的手段，对本地策略、本地日志、核心日志和一切关联的信息都进行加密，甚至是对本地管理员权限也需要一个繁杂的密码来移除限制。当发现未经授权的用户，企图对安全文件删除、修改或改变文件名称时，锁定本地用户并发送一个警报。管理者只能看到和修改他们所拥有组织权限的安全策略。安全审计系统可以做到：如果本地设备被删除或修改了，该系统则可自动进行修复和重建；防止进程关闭技术；进行持续的策略控制，即使某种原因软件没有启动或者终端没有和网络相连，安全策略始终有效；可以阻止试图更改保护者配置日期的企图；提供安全模式操作。

（7）策略控制。全局的策略控制，对某些特殊的部门可以灵活定制不同的安全策略。安全审计系统可以针对一台主机的不同的用户定制不同的安全策略。

（8）整合审计和可检测性，提供审计软件。审计软件能够提供最近六个月所有连接到网络的设备清单，并提供企业终端的安全风险评估。

（9）设备白名单。配合审计软件建立白名单非常便捷。

（10）整合网络管理，支持微软的活动目录管理工具或其它第三方工具。安全策略可以通过活动目录向下分发。

（11）详细的日志和警报管理，日志记录所有端口和设备的活动，供管理员查看和分析。当有报警通过邮件或网页及时通知管理员，并且支持第三方软件。

（12）支持存储设备的只读模式，连接到端口的存储设备可以被设定为只读模式。

(13) 容量控制，可以设置低于规定容量的存储设备的访问。安全审计系统在防止数据偷窃的同时，不影响正常设备的使用。

(14) 复合设备功能确认强制连接设备确认自身功能，只允许经过确认的数据交换。这种措施保证了集成在已确认的惠普打印机中的Flash芯片不会绕开策略导致数据泄漏。

(15) 对终端用户隐藏，策略安装不需要重新启动计算机。系统检测和警告信息只有在有非法操作时才会出现，策略更新和升级被随机执行，以减少网络负担。

四、地级市电子政务外网安全审计的选择

网络中的安全问题其实大部分都是由客户端引起的，所以一定要在运行的前期就部署和设计客户端的审计和控制。如果怕麻烦和工作量大就忽视客户端的审计和控制，这样会完全失去客户端的安全功能，会给后期的网络运行带来极大的隐患和麻烦。安全审计软件有Safend安全卫士、汉邦审计、Lansec等。在选择安会审计软件时，从政策上和功能上都要符合政务网络的建设需求。《电子政务工程技术指南》(国务院信息化工作办公室、科学技术部、信息产业部2003年1月3日共同颁发) 中明确指出“涉及国家经济命脉、信息安全、国计民生和社会安定的电子政务系统，在系统的运行、维护、升级过程中，必要时可要求开发单位提供有关源代码和技术文档支持”，因此，在功能相等的条件下应优先使用国产软件。但是，在功能差距比较大的情况下，有些已经本土化的软件也应考虑，如Safend安全卫士 (Safend是世界顶尖的审计软件，其在国际上大型使用案例非常多，在国内也有很多成功案例)。

地级市政务外网主要是面向民众，突出政务公开，为民办事的电子政府，是面向社会的服务性网络，不在涉密系统范围。因此，选择安全审计系统主要是考虑软件的功能，应从以下几点来比较：

1．运行模式的优劣

首先要比较该软件是运行在用户模式还是运行在内核模式。对于运行在用户模式的审计软件而言，所有信息要全部依靠操作系统的用户接口获得，很容易受到欺骗和攻击，从而失去审计软件的意义；而运行在系统内核模式的软件，属于系统内核驱动的一部分，该软件可直接访问所有系统信息，不会受到欺骗，而内核驱动则保证了审计系统不会受到攻击，因为内核驱动根本没有被攻击的接口。

2．日志记录

日志是审计非常重要的部分，可以说是审计软件的生命，因为它提供给管理员所监控用户的行为记录和统计，是管理员的眼睛和用户行为的原始记录。有的软件只对主机／服务器上的系统日志、安全日志、应用日志进行统一收集，集中管理，这是个极其严重的Bug和错误，是极度危险的。众所周知，操作系统的日志记录除了可以直接删除外，更可以通过日志软件随意修改和删除，这将直接提供给管理者虚假的日志记录，从而失去审计软件的存在意义。任何企图对日志进行的修改都会作为恶意尝试而被记录，这将充分保证了日志这个原始凭据的安全性。

3．伪造设备问题

一直以来，审计软件的一个巨大麻烦，就是如何防止用户伪造设备，比如将Usb无线GPRSModem伪造成Usb鼠标设备 (有相当多的这样的免费软件)。因为审计程序一般都会允许Usb鼠标设备，这样在伪造设备后就可以开辟网上出口，避开系统管理员的检查，导致重要信息泄漏。有的软件由于运行在用户模式，所有信息从操作系统获得，对此毫无办法，无能为力。所以要选取内核驱动模式，且自带协议识别库，直接从底层获得设备，可以轻松地识别出这是个网络设备还是个输入设备，从根本上防止伪造设备通过检测。

4．防篡改机制

有的软件运行在用户模式，它具有以下一些先天缺陷：很容易以安全模式的简单方法通过口令被卸载、通过构件被替换、导致软件崩溃、停止进程，从而失去审计软件的作用。因此，要选择运行在内核模式的软件，它在任何系统模式都不间断地起作用，通过构件的数字签名和冗余的监控机制以及内核模式的结合，完全杜绝系统进

程被停止的危险。

5．功能是否实用，是否严重影响主机的性能和稳定性

有的软件附带了很多的无用功能，如网络监控、邮件监控、文档监控等等。软件功能越多，占用资源就越多，系统潜在的Bug就越多，就越不稳定。同时，由于如此的审计软件要监控很多内容，从而使审计软件成为了主机和网络的累赘。因此，要选择没有垃圾、噱头少、专注于本地计算机的安全审计系统。这样的系统短小精干，占用资源极少；并且其运行异常稳定，系统的体积小，其设置安装简捷。

6．占用内存和CPU的资源

要选择占用内存少，占有CPU资源可忽略不记的产品。

五、小结

网络没有绝对的安全，安全是一个相对的概念。地级市电子政务外网安全审计系统要根据自身安全的实际需要，选择技术、功能等方面符合要求的优秀安全审计软件。对网络系统中的安全设备和网络设备、应用系统和运行状况进行全面的监测、分析、评估是保障网络安全的重要手段。网络安全是动态的，对已经建立的系统，如果没有实时的、集中的、可视化审计，就不能有效、及时地评估系统究竟是不是安全的，并及时发现安全隐患。所以安全系统需要集中的审计系统。在安全解决方案中，跨厂商产品的简单集合往往会存在漏洞，威胁会乘虚而入，危及安全。当某种安全漏洞出现时，如果针对不同厂商的技术和产品先进行人工分析，然后综合分析，提出解决方案，将降低对攻击的反应速度，并潜在地增加成本；如果不能将在同一网络中多个不同或者相同厂商的产品实现技术上互操作，实现集中的审计，就无法发挥有效的安全性，就无法有效地管理。没有实时的、集中的、可视化审计，就不能有效、及时地评估系统究竟是不是安全的，就无法及时发现安全隐患。安全审计系统就可以满足这些要求，可以对网络中的各种设备和系统进行集中的、可视的综合审计，及时发现安全隐患，提高系统安全。

参考文献：

1　徐宜领. 建设电子政务审计监控体系 提高信息安全.[2006-06-17].http://www.cegov.cn/read.php?wid=1103

2　姚国章. 电子政务基础与应用. 北京：北京大学出版社，2002：200 － 201

3　肖德琴. 电子商务安全保密技术与应用. 广州：华南理工大学出版社，2003：242 － 248

4　方雷. 电子政务系统需要全面安全审计. 电子商务世界，2003（5）：28 － 30

作者简介：

高爱乃，男，1953年生；太原理工大学副教授；研究方向：计算机网络、系统集成、智能控制；发表论文10篇，编写教材5本。

SinoEGov 资讯

济南确定“十一五”交通系统电子政务建设目标

“十一五”期间，济南市将继续强化交通信息化建设，优化交通信息中心网络架构，完善交通行业数据库系统，实现全市交通系统电子政务联网，并开发应用公众出行交通信息咨询服务系统。

从山东省交通厅获悉，在日前召开的全市交通系统科技工作会议上，确定“十一五”期间要加强交通基础设施建养技术研究应用，长寿命路面结构研究要走在省内同行业领先行列；大力开展绿色交通技术研究应用，加强交通环保节能新技术、交通建设养护材料再生技术、土地资源合理利用技术研究，推广应用车辆节能新产品，在交通环境评价技术、环境破坏的预防和恢复技术研究方面要取得重要进展。

同时，还将加强交通软科学研究，重点完成公路基础设施投融资管理、运输基础设施建设管理、交通信息化维护管理及行业管理对策等课题研究，为交通各级管理机构决策提供科学依据。

（来源：济南时报）