广西科学院学报
Journal of Guangxi Academy of Sciences

2009,25(4):284~287
Vol. 25,No. 4 November 2009

广西发改委网络信息安全系统设计
Design about the Network Information Security System in Guangxi Development and Reform Commission

李承林,赵 钦,周 丹
LI Cheng-lin,ZHAO Qin,ZHOU Dan

(广西经济信息中心,广西南宁 530022)
(Guangxi Economic Information Center,Nanning,Guangxi,530022,China)

摘要:根据内外网络物理隔离和内外网络数据交换的信息安全防护重点,设计广西发改委网络信息安全系统。该系统除传统的边界保护外,重点解决网络内部防护,杜绝内网非法外联、移动存储介质"摆渡",限制病毒、木马攻击与传播范围。该系统符合网络信息安全保密要求,能够确保信息安全。

关键词:网络信息 安全 非法外联 摆渡
中图法分类号:TP393.08,TP271 **文献标识码**:A **文章编号**:1002-7378(2009)04-0284-04

Abstract:According to the key point of information security protection for physical isolation and data exchange on intranet and internet,the Network Information Security System was designed. This system not only includes traditional frontier protection, but also settles protection of intranet,prevents from illegal connection with intranet from internet,USB ferry and restricts the attack extent from virus and Trojan. This system meets the requirements of Network Information Security and can guarantee the information security.

Key words:network information,security,illegal connection to the internet,ferry

近年来,广西发改委的网络平台经过不断建设与完善,已经具备一定的规模,对广西经济的建设和社会的发展起到了良好的促进作用。但是随着网络信息技术的发展,广西发改委网络平台的信息安全形势变得十分严峻。无处不在的病毒、蠕虫、木马和ARP欺骗等攻击时刻威胁着广西发改委网络平台的正常运行。同时个别工作人员通过拔插网线使用同一台电脑既连接外网又连接内网,以及在内外网间交叉使用移动存储介质,极易造成信息泄密,信息安全得不到很好的保障。为此我们设计一个可防、可控、可信的信息网络平台和纵深立体防御的网络信息安全系统,以保障信息安全。

1 系统设计目标

根据国家保密委员会关于党政机关信息网络、计算机、移动存储介质、涉密载体的使用管理要求和部署必要的网络信息安全技术防护措施要求,借鉴目前业界先进、成熟、可行的网络信息安全技术,针对广西发改委网络信息安全现状和隐患,对严格实行物理隔离的内外网络平台安全系统和内外网络数据安全交换系统进行设计,杜绝内网非法外联、终端非法接入、移动存储介质在内外网"摆渡"、安全审计,同时实现网络边界保护,有效阻止外部攻击;有效隔离病毒、蠕虫、木马、ARP欺骗等攻击,防止网络瘫痪,搭建一个"可防、可控、可信"纵深立体防御的网络信息安全系统,实现"事先预防、事中监控、事后审计"的目标,确保信息安全。

2 系统设计

广西发改委网络信息安全系统包括内网安全管理审计系统、外网安全系统、防病毒系统和内外网数据交换方式4个部分的设计。

2.1 内网安全管理审计系统

传统的网络信息安全系统防护重点是边界,忽略网络内部安全,事实上信息窃取更容易在内部发生。为此,广西发改委网络信息安全系统网络信息安

收稿日期:2009-10-10
作者简介:李承林(1963-),男,高级工程师,主要从事网络信息安全研究。

全的防护重点在网络内部,在内网部署一套内网安全管理审计系统,对内网非法外联自动报警阻断、移动存储介质进行注册管理,杜绝"摆渡"、补丁自动分发、端口流量监控和故障自动定位、终端资源管理、端口控制,行为审计,达到事先预防、事中监控、事后审计的目标,保障网络和信息安全[1]。

如图1所示,内网安全管理审计系统主要包括:内网非法外联控制、补丁分发管理、移动存储介质注册管理、端口流量监控、安全审计等内容。

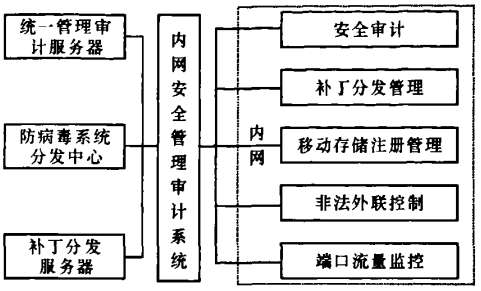

图1 内网安全管理审计系统

2.1.1 内网非法外联控制

内网非法外联控制主要是通过系统控制中心向终端电脑下发安全策略,实时监控终端电脑上网行为,杜绝一台电脑既上内网又上外网,造成信息被窃取,甚至泄密。通过系统控制中心设置终端电脑不允许访问互联网和其他网络,只能使用特定范围的IP地址,同时禁止更改主机IP地址的安全策略。将安全策略下发给终端电脑,并实时监控,一旦终端电脑企图通过拔插网线、多网卡、拨号、代理连接或无线上网等方式非法外联时,依据已经下发的安全策略立即自动阻断非法外联行为并向控制中心报警,同时记录该终端电脑非法外联的日期、时间和访问的网址等信息,该终端电脑自动进入禁止访问所有网络状态。

2.1.2 移动存储介质注册管理

根据权威部门报道,目前移动存储介质在内外网间"摆渡"是信息泄密的主要途径,为此,将本单位凡在内网使用的移动存储介质进行注册管理,限制在特定的范围内使用,禁止非注册的移动存储介质插入内网,同时禁止已注册的移动存储介质在其他网络上使用,杜绝其"摆渡"。利用此功能,将移动存储介质设为特定工作模式(读/写)、授权范围、使用时限等。根据工作性质和信息交换的范围设置移动存储介质只能在特定的IP地址范围、特定的组或特定的终端电脑上使用。

2.1.3 补丁分发管理

由于内网是与国际互联网是物理隔离,因此内网电脑操作系统和其他工具软件无法通过在线自动更新,为了及时堵上系统安全漏洞,提高终端电脑系统安全,在内网上部署一台补丁分发服务器,通过外网下载补丁包,加载到补丁分发服务器,补丁分发中心通过自动检测和分发引擎将终端电脑未安装的补丁自动下发并安装加固,提高电脑防御病毒和木马入侵的能力。

2.1.4 安全审计

安全审计是采用日志方式自动记录终端电脑所有操作行为,包括上网行为、运行状态、补丁安装、端口I/O操作、文件拷贝和资产变更等,为事后审计提供依据。

2.2 外网安全系统

外网安全系统主要包括:网络边界保护、3层网络交换与网络接入认证技术等。外网安全系统如图2所示。

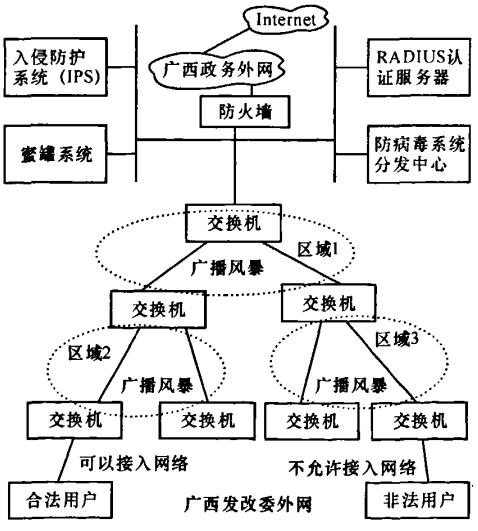

图2 外网安全系统

2.2.1 网络边界保护

网络边界保护是为整个网络平台构筑一道网络"城门",把住进出网络的必经通道。在广西发改委外网与广西政务外网之间部署一台千兆防火墙、在线部署一台入侵防护(IPS)系统和蜜罐系统,通过防火墙、IPS系统和蜜罐系统的相互联动,有效地阻断外部不可信网络对内部可信网络的入侵和攻击。防火墙融合了包过滤和状态检测技术,定期更新安全规则库内容,对网络中的数据流进行监测、限制、阻断等,将不在访问控制列表的IP地址排除在受保护网

络之外，防止各种IP盗用和路由攻击[2]。通过入侵防护系统在线准确监测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断。当入侵防护系统对一些入侵行为不能做出准确判断时，通过一套网络监控系统，实时监控所有进出蜜罐系统的流量，完整地记录下入侵者攻击蜜罐的整个过程，据此修改入侵防护系统规则。通过3者结合与联动有效地防御DDoS、病毒、蠕虫、木马、ARP欺骗等攻击，确保外网信息安全。

2.2.2 第三层网络交换设计

对网络中每一台接入层交换机设置不同的VLAN(每处室1个)并启用动态路由协议(OSPF)，将每个处室设为一个独立区域，每个区域都有自己特定的标识号，每一个独立区域不受其它区域的干扰，核心交换机只负责计算分发独立区域之间的链路状态信息。考虑到网络中某一链路状态发生变化时，会引起整个网络中每个节点都重新计算一遍自己的路由表，这样既浪费资源与时间，又会影响路由协议的性能，因此，当网络中的某条链路状态发生变化时，此链路所在域中的三层交换机重新计算本域路由表，而其它域中三层交换机只需修改其路由表中的相应条目，无须重新计算整个路由表，极大地提高网络交换速度。采用第三层网络交换技术搭建的网络平台能有效地缩小病毒、蠕虫、木马和ARP等对全网络进行广播风暴的攻击范围，把广播风暴主动地隔离在每个区域根节点的网络设备端口上，并即时关闭发起广播风暴攻击的端口，避免网络瘫痪。

2.2.3 网络接入认证设计

采用802.1x协议，基于端口与MAC地址和IP地址捆绑的接入认证控制技术，禁止未经许可的电脑接入网络非法拷贝信息，提高网络信息安全。

对所有接入层交换机端口配置802.1x协议，并在网络中部署一台RADIUS认证服务器，认证服务器的数据库中存放着合法计算机的IP地址和MAC地址，当一台终端电脑用户想接入内部计算机网络时，用户打开802.1x的客户端程序输入用户名和口令，并向认证服务器发起连接请求，当认证服务器收到请求后，将该信息与数据库列表比对，找到该用户对应的口令信息后，用随机生成加密信息发送给请求的客户端程序，客户端收到加密信息后，用该加密信息对自己的口令部分进行加密处理后，传给认证服务器，认证服务器将传送过来的加密口令和自己生成的加密口令进行比对，如果相同，则向交换机发出打开端口的指令，并发送认证通过信息给客户端，允许用户对网络进行接入。反之，认证失败，交换机端口保持关闭状态，不允许用户接入网络。在整个接入认证过程中，所有的加密信息都是不可逆的，杜绝IP地址冒用和电脑非法接入[3]。当一个端口有多用户通过串联HUB方式共享上网时，为每一个用户配置逻辑端口，并对每一个链路进行数据加密，保证各用户之间接入认证的正确性和数据保密性。

2.3 防病毒系统

2.3.1 网络防病毒系统

采用"瑞星网络防病毒系统+360安全卫士"双重防护模式保护桌面终端电脑，启用实时监控中心对病毒和木马程序监控。在内/外网络平台各部署一个瑞星分发中心，每台终端电脑统一安装瑞星防病毒系统客户端软件，实行统一部署、集中防护和管理，同时在每台电脑上安装360安全卫士木马防护软件，实时拦截和查杀木马程序，提高终端用户病毒防护能力，有效地保护网络信息安全。

2.3.2 移动存储介质自动检测系统

病毒通过移动存储介质交叉感染是造成病毒大面积传播的重要途径，为此，在内外网所有电脑上安装一套移动存储介质自动检测系统，对USB端口进行实时监控，一旦移动存储介质接入计算机，该系统立即调用本地防病毒软件对移动存储介质进行查杀病毒，以有效地防止病毒感染计算机，杜绝移动存储介质病毒交叉感染。

2.4 内外网数据交换方式

基于目前网络信息安全严峻的形势，信息泄密的主要途径是移动存储介质"摆渡"，即移动存储介质在内/外网交叉使用，为了有效杜绝此类现象发生，又不影响内/外网数据交换，提高网络信息安全，行之有效的措施是内/外网通过只读光盘进行数据交换，杜绝在内/外网数据交换过程中交换介质被植入特种木马，造成信息被非法窃取，引起信息泄密。内/外网数据交换如图3所示。

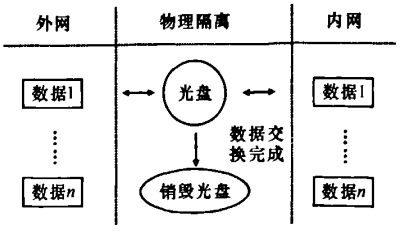

图3 内/外网数据交换

3 结束语

广西发改委网络信息安全系统具有如下主要特

点:(1)网络授权接入访问。采用网络接入认证技术措施,杜绝电脑随意接入网络和访问网络资源的现象,保障网络和信息安全。(2)杜绝内网非法外联和移动存储介质"摆渡"。通过部署内网安全管理审计系统,对内网电脑操作行为实施实时监控,杜绝电脑以任何形式非法外联。通过对移动存储介质进行注册管理,禁止移动存储介质非授权访问,杜绝"摆渡"。(3)病毒有效隔离,避免对全网攻击,造成网络堵塞瘫痪。采用第三层网络交换技术和OSPF路由协议,有效地将病毒和网络广播限制在一个特定区域内,抑制病毒和广播风暴扩散,保护网络安全。(4)事先预防、事中监控、事后审计。对接入网络的电脑实施实时监控,对非法外联、端口流量异常及时报警和阻断,并可以对电脑的端口和外设进行控制,电脑所有操作都留下痕迹,便于事后审计。

广西发改委网络信息安全系统应用实践证明,网络受到病毒、木马的攻击明显减少,杜绝了内网非法外联、移动存储介质"摆渡",很好地解决了内/外网数据安全交换问题,符合网络信息安全保密要求,能够确保信息安全。

参考文献:

[1] 孙玮,何兴高.内网安全监管审计系统的架构设计[J].计算机应用,2008,12(28):267-270.

[2] 蒋明华,李声,李俊.入侵检测系统与防火墙系统联动平台的设计[J].网络安全技术与应用,2009(7):39-41.

[3] 朱海龙,张国清.基于802.1x的以太网接入技术[J].计算机工程,2003,29(18):130-132.

(责任编辑:韦廷宗)

(上接第283页)

由TEA算法[1]来完成。

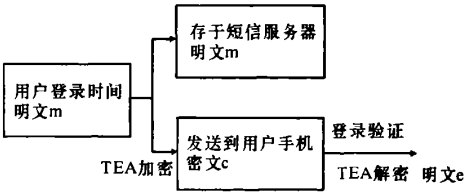

图3 用户的身份认证

3 结束语

为了消除当前企业办公网普遍采用的静态单一口令身份认证机制存在的安全隐患,本文设计一种基于手机短信的一次一用动态口令+用户静态口令的企业办公网身份认证双因子安全体系,并讨论其工作流程和安全机制。手机的普及使该系统具有较高的安全性和使用上的方便性,并且系统通过GPRS MODEM来发送短信息,实现成本低,可与基于互联网的各种应用服务商结合,为其提供安全的用户认证服务,替代传统单一静态口令用户认证方式。同时,在动态口令上采用了TEA加密算法,将密文以短信息的形式发送到用户手机,即使被第三方截获,因其不知道密钥,也无法破解得到相关明文,从而杜绝了非法用户登录办公网的可能,能够极大地提高企业办公网络安全性,可以在企业内进行技术推广和应用。

参考文献:

[1] 杨本臣,张全贵.基于短信息平台的高校办公网络的研究[J].中国科技信息,2007(3):96-98.

[2] 张文.动态口令身份认证系统的设计与实现[J].微计算机信息,2005,21(3):232-233.

(责任编辑:尹 闯)