企业内网安全研究与应用

吴红星,王 浩
(合肥工业大学 计算机与信息学院,安徽 合肥 230009)

摘 要:针对当前企业内网中常见的一些安全问题进行了研究,特别是针对企业无线局域网应用中遇到的新问题进行了分析,查阅相关文献发现现有研究仅在安全域层面提出对策。文中重点对企业内网中的无线网络安全进行分析研究,梳理了企业内网中无线网络建设与使用风险方面的几种类型,找出潜在风险,提出了以网络建设的基础规范为切入点,从根本上解决无线网络安全中的一系列问题,实现企业有线网络、无线网络以及有线和无线混合网络的安全管理。通过精细化的网络管理,对网内IP、交换机Port、终端MAC实行实名分配和绑定,按照企业内部的功能要求,通过在核心层实现严格的VLAN划分和端口准入数配置,实行安全域的访问控制。无线接入点实行动态密码更新,MAC地址自动获取认证,IP可控分配,实现无线设备准入控制。通过行为插件激活无线热点发现来制止USB随身WIFI自建非法AP,消除对企业内网的安全威胁。并验证了解决方案的有效性。

关键词:企业内网;无线网络;网络安全;实名绑定
中图分类号:TP393.1 **文献标识码**:A **文章编号**:1673-629X(2015)09-0154-05
doi:10.3969/j.issn.1673-629X.2015.09.033

Research and Application of Enterprise Intranet Security

WU Hong-xing, WANG Hao
(School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: Study some security problems in the enterprise Intranet in this paper, especially about the new problems in the enterprise wireless LAN application, found that some countermeasures are put forward only in the aspect of security domain according to existing literature review research. Mainly analyze wireless network security in enterprise networks in this paper, combed several types of the enterprise Intranet wireless network construction and using risks, tried to identify potential risk, made network construction basic specification as the breakthrough point, solved a series of wireless network security problems fundamentally, realized the security management for enterprise wired network, wireless network, as well as the wired and wireless mixed network. Through intensification of network management, internal network IP, interchanger port, terminal MAC are all implemented real-name allocation and binding. Implement strict VLAN division and port access number configuration in core layer, to achieve the access control security domain according to the functions of the enterprise. Realize wireless access point dynamic password updating, MAC address automatic access authentication, IP address controlled to allocation, wireless device access control. Also through behavior plug-in to activate wireless hot spots, prohibit the USB WIFI self-built illegal AP, eliminating network security threats to the enterprise. Also verify the effectiveness of the solution.

Key words: enterprise intranet; wireless network; network security; real-name binding

1 概 述

当今时代,随着科学技术的进步和国际互联网的广泛应用,信息化在企业中的作用越来越重要,企业的管理和经营已离不开信息化建设。信息化中的网络建设,特别是企业的内网规划和建设是重中之重。由于企业的内网建设缺少国家层面的统一标准,各企业在建设时都以满足自己的基本日常需求为基准,而较少考虑各类安全问题的影响,尤其是在技术日新月异的当下,各种病毒、各类入侵随时都可能出现。许多企业出现了各种各样的网络安全事故,有的甚至导致了企业的重大经济损失。正是网络安全事故频发,使得企业的内网安全显得尤为重要。今年国家也成立了网络

收稿日期:2014-10-01 **修回日期**:2015-01-09 **网络出版时间**:2015-07-21
基金项目:国家自然科学基金资助项目(61273292)
作者简介:吴红星(1974-),男,博士研究生,教授级高工,研究方向为数据挖掘、网络安全、系统集成;王 浩,博士,教授,研究方向为数据挖掘。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150721.1453.072.html

安全与信息化领导小组,可见国家对网络安全的重视程度已经上升为战略层面。目前互联网的广泛应用和信息系统的建设作为现代企业的管理工具,使很多企业体验到便捷的信息技术带来的价值。国内很多企业都自建了内部局域网,并通过企业内部服务器,共享和使用企业的经营管理等商业数据。企业网络长期、深入的建设与使用,保证了企业的正常生产与经营,随之而来的很多问题也逐渐浮现。文中重点对企业内网中的无线网络安全进行分析研究,梳理了企业内网中无线网络建设与使用风险方面的几种类型,找出潜在风险,提出解决思路,并验证了解决方案的有效性。

经过对比分析,企业内网中网络建设与使用风险主要有以下几个方面[1]:

(1)外来人员(比如客户、合作伙伴)自带的笔记本等接入到企业内部局域网,有意或无意地访问到公司的重要机器或者重要文件,造成泄密隐患;

(2)企业员工有意或无意地修改办公电脑的 IP 地址或 MAC 地址,导致企业内网中的机器 IP 地址冲突,电脑无法上网,影响正常办公;

(3)企业内部员工为了节省数据流量私自拉接无线路由设备,增加内网的非法接入点,导致接入终端不可控和上网行为不可追溯;

(4)企业内部员工利用笔记本电脑的无线网卡通过不安全的 AP 软件做成无线热点,或利用自己的台式机外加 USB 迷你随身 WIFI 做成非法 AP,增加企业内网的非法接入点,导致网上行为不可控。

以上这几种行为导致企业内网存在极大的安全风险和隐患,可能给企业带来巨大的经济损失和商业风险,不利于企业的稳健经营和发展。目前网络调查数据显示我国有近 70% 的企业内网用户处于高度风险的级别,虽然很多企业都表示很重视内网的安全问题,但实际应用中仍然存在一系列的网络安全问题。国家出台的《信息安全等级保护管理办法》明确指出了信息安全等级保护的重点在于内网安全措施的建设和落实。为了有效保护企业内部信息资源和网络应用安全,企业的信息技术部门应当针对以上问题逐一研究,拿出一套可行有效的方案,建立全面的企业内网安全体系,才能为企业的正常办公和生产经营提供良好的内网环境。

2　安全问题分析

人们对网络安全的问题通常关注于病毒和黑客攻击,常规防御的重心都在网络入口,如防火墙、入侵检测、防病毒、漏洞扫描等。这些防御基本上阻止了来自网络外部的攻击,但是来自网络内部的病毒和攻击却层出不穷。通过调研,文中提到的四种行为是企业内网的薄弱环节,应当进行有效管控,否则会导致企业内部网络安全问题,如外设中的病毒入侵、数据被窃取、IP 地址冲突、非法热点成为诈骗的通道等等,这些隐患的问题在文献[2-3]中也有一定的描述。文献[4]针对无线网络的威胁从插入攻击、漫游攻击、欺诈攻击、双面恶魔攻击、窃取网络资源、对无线通信的劫持和监视等方面也做了描述。文献[5]中提到数据若在无线网络上进行明文传输的话,只要凭借一些简单的工具,就可以窃听。企业内部无线局域网除了这些不安全问题之外就是面临病毒的威胁。

目前常用的无线网络标准主要有美国 IEEE 所制定的 802.11 标准,其包括 802.11a、802.11b、802.11g 及 802.11n 等。最常使用有线等效协议(WEP)和保护接入协议(WPA),WEP 是一种相对较弱的无线安全算法,通过 WEP 协议加密的无线网络可提供最低限度的安全,相对来说使用 WPA 协议加密的无线网络则更加安全。企业为了网络安全很多都采取了一些专业方法来进行保护,比如隐藏 SSID 号、MAC 地址过滤等等,这些方法看似安全,实则没有从根本上解决问题。例如,隐藏 SSID 号的方法,通过无线 sniffer 可以将无线网络嗅探出来,因此隐藏 SSID 号方法没有任何安全效果。同样 MAC 地址信息肯定存在无线数据包中的源地址与目的地址信息中,因此入侵者可以很容易获得具备无线接入权限的 MAC 地址,然后通过修改本地网卡 MAC 地址的方法来突破 MAC 地址过滤功能,所以也是不安全的。文献[6]中描述了隐藏 SSID 号、MAC 地址过滤、WEP 加密算法等各种无线网络安全做法中存在的一些问题。

文献[7]提出对于高安全要求的重要网络及大型网络实行 VPN 技术,建设逻辑隧道,对网络层进行身份验证、口令保护和加密,保证移动终端无线接入的安全性,同时便于维护工作站和 AP 的 WEP 加密密钥、AP 的 MAC 地址列表。

文献[8]提出目前的 SSL VPN 和 IPSec VPN 是适合企业使用的两种 VPN 技术。由于 SSL 内嵌在浏览器中,因而任何安装浏览器的机器都可以使用无客户机的 SSL VPN。传统的 IPSec VPN 每一台客户机安装客户端软件;这是因为 IPSEC 协议通过包封装技术,根据 Internet 路由的地址,将内部网络的 IP 地址进行封装,实现异地网络的互通。值得注意的是,这两种 VPN 实现方式都需要与其他无线安全技术相结合,才能发挥系统性的安全效用。

文献[9]提出采用无线入侵检测系统,原先基于有线网络的入侵检测系统具有检测和对已经破坏的系统做出应对的能力。无线网络的入侵检测系统可用来监督和分析内网用户的无线接入活动,对入侵事件的

类型进行判断,对非法的网络行为进行检测,对异常的网络流量进行报警。可以分为集中式的入侵检测系统和分布式的网络入侵检测系统两种。由于无线入侵检测系统是通过提供商来购买的,导致响应不够及时,经常是事后才检测到,适时性不好。

文献[10]认为:企业无线局域网的安全受到局域网整体服务和性能的限制,这是因为企业内网中的无线传输带宽是有限制的,所有用户共享该带宽,由于物理层的消耗,无线网的实际最高有效吞吐量降低为初始设置值的一半。其实无线带宽也可以被如下方式侵占:由于有限网络的网络流量大大超过了无线网络带宽的网络流量;一旦从以太网发送大量的 Ping 流量,就会轻易地侵占无线访问节点里的带宽。如果攻击者在同一无线网络相同的无线信道内发送信号,被攻击的网络就会通过 CSMA/CA 机制进行自动适应,同样影响无线网络的传输;如果攻击者发送广播流量,就会同时阻塞多个无线访问节点;另外,如果传输较大的数据文件或者复杂的 client/server 系统都会产生很大的网络流量[11]。

企业内网基本上是以有线网络为主,无线网络为辅,随着移动互联网的发展、企业的移动协同办公系统的建设和运行、智能手机终端的多样化,很多企业为了办公的实际需求都或多或少搭建了企业内部无线网。绝大多数的企业无线网都是通过账号和密码管理的,缺少或者没有安全的验证机制,导致一个账号和密码所有人都可以接入,遇到问题无法追溯。目前,在有线网络的安全防御方面,由于市面上很多网络安全设备可供选择,例如根据 TCP/IP 协议,监测内网主机的性能、系统资源、状态等,因而相当多的企业对此做得很好,然而在无线网络安全方面,这些企业都显得无从应对。无线网络是企业整体网络不可或缺的一部分,无线网络安全的短板问题,导致企业整体内网安全策略存在很大漏洞。

文中针对企业内网安全存在的问题,提出一种新的解决思路,以网络建设的基础规范为切入点,从根本上解决无线网络安全中的一系列问题,实现企业有线网络、无线网络以及有线和无线混合网络的安全管理。

3 解决思路

结合企业实际情况以及网络完全的保密性、完整性、可用性、可控性、可审查性等,对企业内的各种网络行为进行分析。通过精细化的网络管理,对网内 IP、交换机 Port 等资产进行虚拟化,类似每个员工的终端上网设备,将其作为办公设备被领用,并与其岗位职责、角色建立对应关系,实施基于角色的访问控制[12],由安全管理人员进行管理。在网络核心层按企业内部功能要求通过严格的 VLAN 划分,实行安全域的访问控制,以达到内网中有线网络的设备准入控制。对无线接入点实行动态密码更新,MAC 地址自动获取认证,IP 可控分配,达到无线设备准入控制的目标。对所有外来的人员上网实行实名登记,并对自带的终端设备进行 MAC 地址自动获取后绑定分配的 IP 地址上。另外在外来人员使用的终端上安装行为控件,当出现异常情况时,可以切断该用户上网功能。

在文献[13]里利用 VLAN 技术,通过配置网络及安全设备的访问控制列表等手段将划分出来的各个安全域隔离等有描述,但只是基于 VLAN 层面的,没有在用户终端设备和端口层面进行研究。文中提出对企业内部局域网的所有电脑设备都实行 MAC 地址、IP 地址绑定接入层交换机 Port,并按照 VLAN 的划分管理,接入到不同的 VLAN。当企业外来人员需要接入公司有线的内网时,可以按照就近原则,由对应部门提出申请然后接入其部门 VLAN 里,并将外来人员电脑设备的 MAC 地址、以及临时分配的 IP 地址绑定接入层交换机的 Port(每个部门都预留 30% 的端口和 IP 地址),或者独立划分出一个临时 VLAN,按照工作需求进行 VLAN 之间的访问控制。针对需要从企业无线接入点接入的外来人员或者企业内部人员无线的设备,在核心交换机里配置一个无线专用 VLAN,并限制接入设备数,动态密码更新,MAC 地址的自动获取认证,这样既可以满足企业实际工作需求,又能有效控制 IP 地址冲突,杜绝影响办公以及信息外泄后不可追溯等问题。还有从加密认证[14-16]的角度对无线局域网安全机制进行研究。

本方案将企业员工的实名、接入交换机 Port 号、VLAN 号、MAC 地址、IP 地址等绑定在接入交换机 Port 上,并在交换机上配置接入最大数为一,同时加入准入机制,制止了员工私接路由设备做非法 WIFI 热点的问题。

针对前文提到的安全风险中的第三和第四类问题,查找了相关文献,未有相关报道,文中进行了大量的研究和实际测试,发现通过上网行为设备进行控件布防,在上述方案的基础上启用受控插件的无线热点发现等功能完全可以解决。

4 实现方法

网络安全是网络上的信息安全,信息安全包括通信安全、计算机安全、网络安全三个阶段。网络安全目的是解决在分布网络环境下对信息载体及其运行提供安全保护问题,使网络系统的硬件、软件及其系统中的数据受到保护,不因偶然或恶意的原因而遭受破坏、更改、泄露,系统连续、可靠、正常地运行,网络服务不中

断。网络安全的属性具备信息的保密性、完整性、可用性、真实性和可控性等。网络安全具体就是包含网络设备安全、网络信息安全、网络软件安全。网络完全应遵循可控和可追溯性原则。

企业内网的所有行为应该符合以上这些条件才是完备的网络环境。

4.1　综合布线工作

按照网络架构,企业中心机房和各楼层网络部署分属于核心层和接入层(根据企业实际情况也可以增加汇聚层)。办公房间的有线部署按照如下方式进行:各楼层部署一台接入层交换机,每个办公房间根据实际的人数布线并预留 2 个备用点,所有楼层接入层交换机端口的数量全部按照 25% 的冗余预留。每个接入层交换机通过光缆接入核心交换机或者汇聚层交换机。核心交换机做成双机互为热备。会议区、公共走道区无线部署策略如下:根据会议室的面积大小进行 AP 的选择,所有的 AP 按照中继模式链接,然后接入 POE 交换机,再接入上网行为管理设备。此有线和无线网络的部署方案既解决了网络验证的问题,也保证了所有区域的无线网络名称唯一性,后台对无线覆盖的区域可以随时开启和关闭网络。

4.2　按照企业的部门规划出 VLAN

借助于企业的内部组织机构可以迅速将企业内部职能 VLAN(虚拟局域网)进行划分。划分 VLAN 后,便于标识定位实际组织中的人,并有利于随时建立很多的虚拟组织。每个 VLAN 在交换机里进行命名,也极大地方便了网络后台人员的管理。

VLAN 划分表见表 1。

表 1　VLAN 划分表

序号	部门	VLAN 号	备注
1	公司领导	100	虚拟部门
2	综合部	101	
3	人资部	102	
4	财务部	103	
5	投资部	104	
6	信息部	105	
7	党群部	106	
8	审计部	107	
9	临时部	108	外来人员专用

4.3　VLAN 的配置

按照划分的 VLAN 进行核心交换机的配置,同时按照部门的人数,每个人分配一个接入层交换机 Port,在核心交换机和接入层交换机上进行配置。核心交换机上的 VLAN 配置如下:

```
HSGroup-4506_A#
Valn database
HSGroup-4506_A(vlan)#
vlan 100 name gongsilingdao
HSGroup-4506_A(vlan)#
vlan 101 name zonghebu
HSGroup-4506_A(vlan)#
vlan 102 name renzibu
HSGroup-4506_A(vlan)#
vlan 106 name dangqunbu
HSGroup-4506_A(vlan)#
vlan 107 name shenjibu
HSGroup-4506_A(vlan)#
vlan 108 name linshibu
```

在接入层交换机上进行 Port、IP、Port 接入最大数配置:

```
HS-2960_6_1(config)#
HS-2960_6_1(config)#
HS-2960_6_1(config-if)#
interface FastEthernet0/13
description (506-2)zhanghuili
switchport access vlan 105
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address eca8.6bc6.81e8
ip access-group 1413 in
HS-2960_6_1(config)#
access-list 1413 permit 172.16.104.136
```

以上配置是按照 VLAN 划分表对 VLAN 号进行命名,然后对交换机端口进行描述,确保交换机端口和办公房间墙上的网口号一一对应,并绑定终端的 MAC 地址、IP 地址等。后台可读性强,并完全做到访问可控。

4.4　无线接入点的管理

在无线接入点(AP)对应的端口实行动态管理,使用具有 WPA 协议的 AP 设备,按照人数配置 IP 地址上限数,如有人需要用无线网络,就临时开通,实行密码的动态管理更新。同时进行 MAC 地址的获取和实名注册。确保做到实名接入,待使用结束立即 down 掉 AP 对应的接入层端口,完全规避网络 sniffer、WPA 加密破解等不安全行为的发生。针对非法的无线接入点(AP),一旦发现就必须立即终止其在网络中的运行,否则别人通过这个非法 AP,可以接触到数据库和文件服务器等企业内网中的重要资源[1]。为了杜绝非法 AP,除了上述的方法外还可以在企业防火墙后串入上网行为管理设备,并按照划分 VLAN 的组织结构在上网行为管理设备中进行配置,激活行为管理中的无线热点发现功能,同时在企业内网使用的 PC 终端部署行为插件,按照企业的各种制度要求进行相关策略的

部署和下发。在 PC 终端内部就可以检查数据包,区分哪些是通过类似 USB 随身迷你 WIFI 自建的非法 AP 接入的 Android、iphone、ipad 等移动终端设备,发现有尝试连接行为就立即断网,此种方法可以把威胁控制在事前,确保了企业网络的安全。

5 结束语

每个企业都有自己的实际网络应用情况,只有具备了保密性、完整性、可用性、可控性、可审查性的网络才是完整和安全的。文中针对目前企业面临的实际问题进行应用研究,从安全的角度对精细化管理网络安全进行了阐述,梳理了存在的问题,提出了解决问题的思路和方法,并进行了实际测试,结果证明该方法是行之有效的。文中既解决了企业内网中有线网络的常见安全问题,也解决了企业内部无线网络的安全难点问题,特别是解决了非法接入点,以及 USB 随身迷你 WIFI 自建的非法 AP 给企业网络安全带来的威胁等问题。文中的方法在企业实施后,企业内部网络运用效果良好。

参考文献:

[1] Park J S, Dicoi D. WLAN security: current and future[J]. IEEE Internet Computing, 2003, 7(5): 60-65.

[2] 朱 敏. 非法无线设备管理[J]. 网络安全技术与应用, 2007(11): 91-93.

[3] 贺婷婷. 基于 TCP 本地延迟抖动的非法 AP 检测方法研究[D]. 长沙: 湖南大学, 2008.

[4] 实现无线网络安全的途径和方法[J]. 计算机与网络, 2012, 38(16): 43-43.

[5] 给企业无线局域网组建的一些建议[EB/OL]. 2010. http://www.bitscn.com/network/wireless/201001/179926.html.

[6] WPA 加密被破解 无线安全路在何方?[EB/OL]. 2008. http://sec.chinabyte.com/400/8649400_2.shtml.

[7] 陈 玮. 企业无线网络移动办公的安全接入问题分析[J]. 信息通信, 2013(3): 239-239.

[8] 彭 州. 无线局域网的安全威胁分析及防范措施[J]. 金融科技时代, 2014, 22(3): 87-88.

[9] 陈 凯. 企业无线网络常见的威胁及其应对措施探索[J]. 无线互联科技, 2012(11): 66-66.

[10] 杨雅静. 常见无线局域网设置安全的几种隐患[J]. 电脑知识与技术, 2011, 7(14): 3272-3273.

[11] 无线局域网的安全分析及防范措施[EB/OL]. 2013. http://network.chinabyte.com/377/12529377.shtml.

[12] Sandhu R S, Coyne E J, Feinstein H, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38-47.

[13] 范 菁, 祁 悦, 李恒志. 计算机局域网安全域划分浅探[J]. 中国无线电管理, 2003(11): 35-36.

[14] Tseng Yuh-min. USIM-based EAP-TLS authentication protocol for wireless local area networks[J]. Computer Standards & Interfaces, 2009, 31(1): 128-136.

[15] Chandramathi S, Arunkumar K V, Deivarayan S, et al. Modified WEP key management for enhancing WLAN security[J]. International Journal of Information and Communication Technology, 2008, 1(3/4): 437-452.

[16] Chandramathi S, Arunkumar K V, Deivarayan S, et al. Fuzzy based dynamic WEP key management for WLAN security enhancement[C]//Proc of international conference on communication systems software and middleware. [s. l.]: [s. n.], 2008: 409-414.

企业内网安全研究与应用

作者： 吴红星， 王浩， WU Hong-xing， WANG Hao
作者单位： 合肥工业大学 计算机与信息学院,安徽 合肥,230009
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(9)