企业无线网络安全设置

随着网络技术的不断发展，有线网络已经不能满足现代化企业的办公要求，而无线网络由于不受网线和地点的束缚，越来越受到了人们的青睐。但是企业网络不可忽视的重要的两点就是安全性和稳定性，所以对于无线网络的一些安全防护，就是必不可少的了。

入侵无线网络的方式

要想对企业的无线网络进行周密防范，必须了解企业无线网络存在的安全隐患。在日常使用中可以发现，企业无线网络的安全隐患主要有以下几种情况：

1、无线网络不设防

由于很多企业对无线网络并不了解，加之网络安全意识的缺乏，在部署无线网络时，很多网管人员并没有对无线网络设置进行相应的安全设置。众所周知，如果无线路由器不进行设置，用户在无线网络覆盖范围内就可以接入企业的无线网络。通过无线网络接入设备，入侵者可以掌握到该企业非常全面的网络信息。

由于企业网管人员没有对无线网络设备进行任何设置，无线网络将一直保持厂商出厂时的默认设置。无线路由器的地址是厂商默认的，用户名和密码都是默认的，在信息发达的互联网中，稍微具备一点网络知识的人就可以轻松查找到各品牌无线路由器厂商的默认设置，这使得企业的无线网络处在不设防的状态。

2、无线网络设置漏洞

目前，企业无线网络的搭建，都是基于无线 AP、无线路由器及无线网桥等设备，而且其网络覆盖范围有限。正因为无线网络的覆盖范围有限，一些企业的网管人员在搭建无线网络时忽视了无线网络的安全。

无线网络接入与有线网络最大的不同是，无线接入无需在企业的交换机或路由器等网络设备上插上网线，只要有无线网络信号，用户就可以接入企业的无线网络。无线路由器的设置口令，DHCP 服务器，无线网络的 SSID 号码，这些都是无线网络存在的安全漏洞，入侵者通过这一系列的信息可以轻松进入企业网络。除此之外，一些企业的无线网络都没有进行数据加密，这也是企业无线网络的另一漏洞。除上述两种漏洞之外，无线网络设备通常也会存在一些安全漏洞，这些都是为入侵者打开的大门。要想打造一个安全的企业无线网络，网管人员必须针对这些安全漏洞做出相应的防范措施。

企业无线网络周密设防

1、给无线网络设备加把锁

通常情况下，入侵者先是获取无线网络设备的权限，因为无线网络设备中存放着企业的网络信息。很多安全意识缺乏的网管人员，认为无线网络设备并不涉及企业网络的核心，搭建无线网络时并没有对无线网络设置的默认用户名和密码进行更改，这无疑成为企业无线网络的最大安全漏洞。为此，要想保障企业无线网络的安全，必须将无线路由器或无线 AP 等网络设备的默认密码更改掉，对于支持更改用户名的网络设备，强烈建议把设备默认的用户名更改掉。在设置无线网络设备的密码时，最好使用字母和数字相混合的密码，并且要定期更换密码。

2、关闭无线路由器的 SSID 广播

SSID(Service Set Identifier)也可以写为ESSID,用来区分不同的网络,最多可以有32个字符,无线网卡设置了不同的SSID就可以进入不同网络,SSID通常由无线路由器广播出来,通过XP自带的扫描功能可以相看当前区域内的SSID。简单说,SSID就是一个局域网的名称,只有设置为名称相同SSID的值的电脑才能互相通信。只要知道了企业无线网络的SSID号,入侵者就可以轻松接入企业的无线网络。

在默认情况下,无线路由器的SSID是路由器的品牌名称,而且是默认的,例如,TP—Link无线路由器的SSID号默认为“TP—Link”,这无疑给了入侵者一个最佳的机会。为此,我们必须将无线路由器默认的SSID号更改掉。为了安全,强烈建议用户关闭无线路由器的SSID广播。为了保障企业无线网络的安全,建议定期更改无线路由器的SSID号。

3、禁用无线路由器的DHCP服务

从表面看,DHCP服务与企业无线网络的安全风马牛不相及,殊不知,DHCP服务会暴露企业网络的一些信息,这对于企业无线网络的运行是一个不小的威胁。

究用户接入企业无线网络的过程不难发现,用户使用无线上网时,无线路由器就会自动分配一个IP地址给无线网络客户端,这样,无线客户端就会从无线路由器中获得IP地址、子网掩码、DNS及网关等信息。获得了IP地址等一系列的信息之后,无线路由器无疑将会暴露于公众之下,入侵者很轻易的就可以使用无线路由器的资源。为此,启用DhpC服务器会降低企业无线网络的安全系数,成为一个有隐患的漏洞。为此,要想保障企业无线网络的安全,必须禁用无线路由器的DHCP服务。

4、开启无线上网加密设置

无论是无线路由器还是无线 AP，其设置中都提供了无线上网加密设置。设置了无线上网加密之后，无线客户端必须凭密码才可以接入企业的无线网络。经过无线上网加密之后，入侵都将无法搜索到加密的无线网络信号，这样可以大大增加企业无线网络的安全性。

目前，无线网络设备提供的无线上网加密设置，通常有 WEP、WPA/WPA2 和 WPA - PSK/WPA2 - PSK 几种模式。在上述的加密模式中，WEP 是最简单的加密方式，建议有条件的企业采用安全级别相对高的加密模式。

5、善用无线路由器的安全设置

在一些品牌的无线路由器中，诸如“硬件防火墙”及“高级安全设置”已经是基本组件。通过“硬件防火墙”，可以对 IP 地址及 MAC 地址进行限制，防止非法用户入侵。众所周知，每台机器会拥有一个唯一的 MAC 地址，企业的网管人员可以允许本企业的 MAC 地址使用无线网络，这样，入侵者就很难再入侵到企业的网络中。

6、无线路由器的 MAC 地址绑定

一些高档品牌的无线路由器产品的安全设置中，提供了 MAC 地址绑定的功能，绑定了 MAC 地址后，其他 MAC 地址的机器就无法使用该无线网络。除此之外，无线路由器还拥有更多的安全设置，网管人员可以根据自己企业的需求进行相关的设置，打造一个安全的企业无线网络应用环境。目前，即便是最低端的无线网络设备，都提供了“软件升级”功能，为了让企业的无线网络更加安全，用户可以定期升级无线网络设备的软件。

在日常应用中，企业无线网络安全是一个涉及多方面设置的综合问题，而且非常复杂。为此，企业网管人员必须周密防范，把好企业无线网络的大门。更重

要的是，企业网管人员要时刻紧绷安全这根弦，切不可对企业无线网络安全掉以轻心！