

办公网络安全风险浅谈

安 亮

陕西省铜川市烟草公司，铜川

摘 要 | 随着社会科技不断发展，网络与人的关系越来越紧密，而办公网络也随之诞生。通过网络的使用，带给人们的是工作生活上的快捷方便，而办公网络的安全隐患也随之而来。企业的数据、个人信息、系统数据等等。本文就实际工作中遇到的及处理的一些网络安全问题，从安全角度展开探讨。

关键词 | 办公网络；安全风险；防范措施

Copyright © 2021 by author (s) and SciScan Publishing Limited

This article is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/). <https://creativecommons.org/licenses/by-nc/4.0/>



1 前言

在当前的信息时代下，网络随着科技发展深入到千家万户。各个企业也根据自身的需求，搭建自身的办公网络，方便自身的业务开展及对外交流。这种方式有利于公司自身的资源整合，各部门之间工作协同，能够提升工作效率，也有利于跟外界的相互交流。但是随着办公网络的使用，各种不安全因素也随之而来^[1]。

作者简介：安亮，男，1989 年 3 月出生。本科，计算机技术与应用专业，陕西蒲城。研究方向：网络管理及系统管理。

文章引用：安亮. 办公网络安全风险浅谈 [J]. 现代计算机技术与应用, 2021, 3 (2): 1-5.
<https://doi.org/10.35534/mcta.0302006>

2 企业办公网络中会出现的不安全因素

2.1 IP 方面

IP 协议^[2]主要用于异构型网络之间的相互连接和路由选择，例如将 WAN 与 LAN 互联。在网络中，IP 是每个网民的身份名片，都是独一无二的，一旦自身的 IP 地址泄露出去，不法分子就可以利用这个 IP 通过一些手段获取你电脑上的数据、信息。另外由于一些员工在使用电脑时使用自动获取 IP 地址，会产生 IP 冲突问题无法访问网络，对工作、生活等造成不便和不必要的麻烦。

2.2 私自架构 WIFI 网络

WiFi^[3]是在当前信息网络中不可或缺的一部分，WIFI 网络构建简单、使用方便对企业的业务开展以及部门交流，工作协同方面带来了极大的方便，但是带来方便的同时也带来了安全方面的隐患，比如通过 WIFI 连接进入网络之后，在网络中释放电脑病毒或木马，更有甚者直接对 WiFi 本身做手脚，一旦连接到动了手脚的 WiFi 后，那么不法人士就可以通过 WiFi 直接获取你的账号、密码等等。

2.3 个人电脑弱口令

弱口令^[4]指的是仅包含简单数字和字母的，容易被人猜测出来的简单口令，比如生日、简单的顺序数字或字符，如 123、23456、abc 等等，弱口令的设置是由于人的惰性导致的，随着信息系统的普及，每个人使用的账号，口令少则三五个，多则十几个，弱口令设置简单，记忆方便，所以被大量使用。但是在方便使用的同时也非常容易被人猜测到，更容易被暴力破解。我国在 2019 年处理的安全事件中，弱口令事件占比达到了 35.1%。

3 企业办公网络中不安全因素的防范

3.1 关于 IP 的问题

IP 地址的问题需要解决的是 IP 地址管理的问题，首先要对员工进行培训，让大家提高网络安全意识，让员工明白 IP 地址的意义及个人不要随意更改 IP 地址。其次信息中心人员应该对 IP 地址的使用做好规划，对 IP 地址与人员做好一一对应，设备的 mac 地址与 IP 地址做好绑定，做到一人一设备一 IP 地址。保证在发现病毒或者木马传播时能够迅速找到源头，进行紧急处理。

3.2 私自架构 WIFI 网络

关于私自架构 WIFI 的问题，要在加强办公网络管理的同时，做好员工网络安全思想教育，让员工了解私自架构 WiFi 的危害性。同时信息中心对办公网络环境中的 WiFi 进行路由管理，比如禁止 WiFi 设备访问办公系统，对 WiFi 设备的密码设置为数字加大小写字母及符号的复杂密码，并且定期进行更换。防止有外部人员通过 WiFi 进入公司内网。

3.3 弱口令问题

弱口令问题一直都是让网络管理员比较头疼的疑难杂症。在日常应用中的网络设备、各类通过网络进行数据传输的物联网探测器等都是需要通过口令验证才能进行访问的，设备厂商一般会在出厂时给设备设置一个统一、简单的访问口令（弱口令），需要用户在实际使用时对口令进行更改，以达到信息安全的效果。因此，口令使用的关键还在于系统使用人员，要避免弱口令的使用首先还是要对员工进行网络安全培训，提升员工网络安全意识。其次可以制定严格的规章制度，要求每名员工的口令符合大小写字母、数字加符号的组合，规范账号密码的使用，对自己使用的账号密码进行保密，不将自己的账号密码随意外泄等等，另外网络管理员可以通过技术手段对弱口令进行筛查，强制使用人员对密码进行复杂化设置并且定期进行更换。

3.4 效果

上面所述的三个问题都是在实际工作中经常遇到的，而我通过这些方法减少了问题的发生，提高了工作效率，保证了部门之间的正常沟通协调，也减少了信息的泄露的可能性。

4 结语

办公网络在信息爆炸的时代里，随着科技的发展会越来越迅速，也越来越专业，体现出办公网络的快捷性，简易型，易操作性。系统更加完善，可操作性越来越强。本文通过在日常工作中出现的一些问题向大家浅显的做一表述，通过本文的介绍，企业要对网络进行优化、完善的同时，绝不能忽视员工素质的培养，通过制度制定及执行、员工素质教育，切实提高员工网络安全意识，切实保障办公网络安全可靠^[5]。

参考文献

- [1] 陈斯讯. 筑牢网络安全防火墙 [J]. 企业管理, 2020 (2).
- [2] 蔡忠见. IP 协议的分析的 IP 技术的发展 [J]. 渝州大学学报 (自然科学版), 2002 (2).
- [3] 田延伟, 杨松如, 李杰. 无线 WiFi 密钥 APP 风险隐患及对策研究 [J]. 信息网络安全, 2017 (7).
- [4] 吴思琪, 吴小岭. 解决大批量部署的网络设备弱口令问题的方法 [J]. 电脑编程技巧与维护, 2019 (8).
- [5] 魏玉峰. 浅析远程办公网络安全风险与防护措施 [J]. 网络安全技术与应用, 2020 (4).

On the Risk of Office Network Security

An Liang

Tongchuan Tobacco Company, Tongchuan

Abstract: With the continuous development of social science and technology, the Network More and more close relationship with people. And the office network was born. through the use of the network What it brings to people is the quickness and convenience in work and life. And the security risks of office network also follow. Enterprise Data, personal information System Data Wait. This article on the actual work encountered. And deal with some network security issues. Discuss from a safety perspective.

Key words: Office network; Security risk; Precautionary measures