

关于提高电力系统计算机网络信息安全水平的研究

高 静 孙常鹏 王 银

国网天津市电力公司信息通信公司天津 300010

DOI:10.18686/dljsyj.v1i3.1123

【摘要】近年来,我国一直在不断改善电力系统的技术设备。就是为了更好的适应当代信息化社会的不断发展,为适应信息技术的飞速发展,也完善了电力系统的计算机网络化管理,但是在管理的过程中却也存在安全的问题。想要确保电力系统计算机网络信息的安全顺利进行,还需进行科学化的管理工作,不断加强电力系统计算机网络新的规范制度,最终实现电力系统计算机网络信息能够在我国更顺利稳定的发展。

【关键词】电力系统;计算机网络;信息安全

引言

目前,随着电力系统计算机信息的不断发展,难免存在一些安全隐患,所以要不断加强对电力系统计算机网络信息的管理工作、更加完善安全运行及操作管理、企业投入更多的资金支持电力系统计算机网络信息风险的防范及加大系统运行,才能确保电力系统计算机网络信息安全、稳定的运行,并将其发挥到最大作用。我国信息安全产业最重要的一部分就是电力系统信息网络,但我国的研究水平有限,还需要不断向发达的地方学习计算机网络信息安全方面的技术。

1 计算机信息安全的概述

(1)很多发达国家无论政治还是经济文化都在用计算机信息的基础设施,相应而生的也有很多的黑客对信息进行攻击,现代的信息技术就是新的作战技术,在目前的大环境下,各国面临的最大的挑战就是计算机信息安全问题。因此,我国还需不断加强对计算机信息安全的科技能力。1990年,英、法、荷兰等欧共体国家联合发布了关于信息技术安全评估的准则^[1]。1991年,有一部关于计算机信息安全方面的法则在我国颁布。自从法则颁布,很好的促进了我国计算机信息安全的快速稳定发展。目前我国需要研究更多的关于计算机信息安全方面的管理内容,例如,关于风险管理的规范、设计到的业务范围以及一些数据的管理等等,还需要对业务进行统一的规范,不断建立更安全的支撑平台。

(2)2001年,国际组织发布了计算机网络信息安全的《信息安全管理实施指南》,这则指南讲述的就是各个国家有必要构建一个关于计算机信息安全方面的管理平台,有了这个平台,计算机信息就多了一

层防御。这一畅想也促织我国的计算机信息安全风险管理更上一个台阶,使其进入了深层次研究的阶段^[2]。

2 威胁电力系统计算机网络信息安全的主要攻击手段

2.1 口令攻击

一般情况下,黑客主要用口令攻击,利用口令进入对方的系统,从而盗取到自身需要的数据信息等。黑客首先要确定攻击对象,利用抓包技术将数据拦截下俩,通过“字典”穷举,多次用口令测试网络系统,最终将系统利用口令攻破,这样得到正确的口令。口令攻击在UNIX系统入侵和攻击过程中,UNIX系统一般不会再界面显示成功还是失败,计算机系统也封锁不了黑客,黑客可以在系统多次试验自己编写的口令,直到口令测试成功,进入系统,黑客通过Telnet、FTP等程序,这些程序能破解盗取的加密的一些软件,不仅达到盗取计算机信息的目的,还能破坏计算机的系统^[3]。

2.2 网络窃听、数据劫持攻击

黑客最常用的盗取计算机信息,破坏系统的方式就是网络窃听,和在传送中截取计算机数据。网络窃听、数据劫持攻击一般都是在进行数据传输时才会出现,在信息进行终端传输时,一些黑客利用这两种方式开始截取自身需要的计算机中的信息数据。黑客一旦操作成功,再利用Elcomsoft Wireless Security Auditor软件把得到数据进行破解,最终得到计算机用户的各种信息。获取密码信息后,一般还可以根据已经获得的信息进行二次攻击,盗取其他数据。

2.3 IP欺骗攻击

黑客能获取到计算机的信息,主要是获取了对

方的 IP 地址,黑客利用探测技术,有了 IP 地址就能攻击系统的内部。电力系统计算机网络受到 IP 欺骗攻击后,系统会自己断开网络连接,这时计算机就没法在进行联网。在进行 IP 欺骗攻击时,会在 IP 协议上看到报文。黑客还可以利用 IP 协议传送报文时伪装网络主机,通过复制以前的统 TCP/IP 地址,骗取返回报文,最终实现黑客攻击的目的,还能造成网络冲突,破坏系统的网络,卒中实现截取信息的目的。

3 提高电力系统计算机网络信息安全之思

3.1 完善电力系统工作环境

电力企业应该投入一定的资金支持电力系统外部硬件设施。一方面,应该增加外部的监控的设备。不仅增加一些电子摄像头,还要设置好摄像头的警报系统,增加进入机房权限的功能。可以设置指纹,利用指纹的设置限制无关人员进入机房。根据机房内部设备的设置位置,合理设计消防设施、应急设施的分散安装趋区域,保证电力系统计算机网络机房受到威胁时可以有最快的速度投入使用^[4]。另一方面,还应该改善员工的工作环境。在正确的位置放入一些硬件的设备,把主机箱的权限进行限制,避免一些无用的病毒侵入到系统的主机箱,最终破坏电力系统计算机网络信息的安全。此外,一定要做好电力系统的线路设置,要准确、有序的找出系统中存在的问题。

3.2 规避电力系统网络漏洞

①管理人员管理好系统的 IP,黑客确定目标主要通过 IP 地址,黑客都是利用网络探测系统实现对电力系统的攻击的。所以企业应该管理好自己的 IP 地址,而且要隐藏好 IP。在进行 IP 隐藏的时候需要用中介物质,比如运用代理服务器。有了代理服务

器,就能阻碍黑客探测代理服务器的 IP,这样也能组织黑客攻击电力系统网络服务器。此外,可以在计算机端口安装一个监视的程序,这样能对黑客入侵系统的时候增加一层防御能力。②建立防火墙以及防病毒系统,对于电力系统计算机网络安全来说,防火墙在阻止黑客入侵以及系统文件备份上都有着重要的作用^[5]。防火墙软件的设置在电力系统也很有必要。

3.3 提高网络维护人员综合素质

要想提高电力系统计算机网络信息安全的技术,就要不断培养相应的技术人员。作为网络维护人员,必须正确认识自己的职责,不能再计算机系统插入电子介质,严格按照各项标准进行系统的更新和检验,定期对系统进行维护。企业可以增加培训课程,增强维护人员的意识。并且组织培训和各种考核,对一些基本的知识不断给维护人员进行强化。严格要求员工在进行系统维护时删除没用的东西。利用培训,增加维护人员的技术水平,培养更多的网络技术人才。

4 结语

虽然我国的电力系统计算机信息化管理进行的比其他国家晚,所以在使用过程中还有很多不完善的地方,所以,我国还需要不断完善和加强电力系统计算机网络信息化管理建设安全的风险管理的工作。我国需要不断增加对对计算机网络信息化管理的管理工作,增强操作管理和安全运行,投入更多的资金在建设计算机网络信息化管理上来。这样才能更好的保证计算机网络信息的安全、顺利进行。此外,当计算机网络信息化出现什么问题时,一定要及时提出解决方案,促进我国计算机网络信息化管理更好的发展。

【参考文献】

- [1]李岳泽.关于提高电力系统计算机网络信息安全水平的研究[J].科学技术创新,2018(22):88-89.
- [2]伍慧.关于提高电力系统计算机网络信息安全水平的研究[J].数字通信世界,2018(06):263-264.
- [3]李世昫.关于提高电力系统计算机网络信息安全水平的思考[J].通讯世界,2018(05):224-225.
- [4]李斌.关于提高电力系统计算机网络信息安全水平的研究[J].电子技术与软件工程,2015(21):214.
- [5]景志高.关于提高电力系统计算机网络信息安全水平的研究[J].硅谷,2014,7(08):163+162.