变电站自动化系统安全问题探讨

魏世贵,陈朝恒
(南京南瑞集团中德保护控制系统有限公司,江苏 南京 210061)

摘 要:对目前变电站自动化网络信息安全存在的问题进行分析,提出边界防护与内部防护相结合、硬件与软件防护相结合的方法,保障变电站自动化系统安全稳定运行,并给出了具体措施。

关键词:变电站自动化系统;信息安全;防护
中图分类号:TM76 **文献标志码**:B **文章编号**:1009-0665(2010)03-0060-03

随着电力系统的网络化程度不断提高,电力系统的安全问题引起了国家相关部门的高度重视。国家电力监督委员会适时发布了《电力二次系统安全防护规定》及《全国电力二次系统安全防护总体方案》等有关文件,各电力企业据此进行了相关的安全防护工作。变电站自动化系统安全稳定的运行是电力自动化系统的重要组成部分,它对整个电力系统起着重要的作用。

1 边界安全防护

在变电站二次系统中,根据系统的特点、重要程度、数据流程、安全要求等,一般将变电站自动化系统划归为生产控制区,其中包括控制区(安全区Ⅰ)和非控制生产区(安全区Ⅱ)。控制区的业务系统或功能模块的典型特征为直接实现实时监控功能,是电力生产的必备环节。系统实时在线运行,使用调度数据网络或专用信道,典型应用包括监控系统、五防系统、安控装置、保护装置及保护设置工作站等;非控制生产区,典型应用包括故障录波系统、电量计费系统等。生产控制区同时会与安全区Ⅲ即管理信息区有着密切联系。

现阶段运行变电站二次系统都为独立网络,一般和外界隔离运行,但随着电力调度数据网络的广泛应用,其边界安全防护功能显得更加重要。根据电监会《电力二次系统安全防护规定》中提出的变电站二次系统安全防护应遵循"安全分区、网络专用、横向隔离、纵向认证"的原则,需对不同分区采用不同的安全防护等级和防护水平。因此变电站自动化系统中控制区和非控制生产区之间须采用经有关部门认定核准的硬件防火墙或相应的设备进行逻辑隔离,应禁止E-mail,Web,Telnet,Rlogin等服务穿越安全区之间的隔离设备。安全区Ⅰ,Ⅱ与安全区Ⅲ之间应该采用经过国家有关部门认证的电力专用单向安全隔离装置。各单位应严格禁止E-mall,Web,Telnet,Rlogin等网络服务和以B/S或C/S方式的数据库访问功能穿越专用安全隔离装置,仅允许纯数据的单向安全传输。其总体安全防护策略如图1所示。

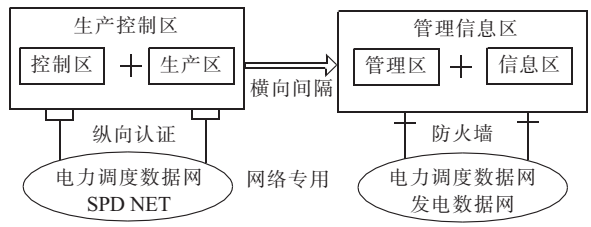

图1 电力二次系统安全防护策略

由于各电力企业对电力系统安全问题越来越重视,网络安全隔离装置和纵向认证加密网关已经得到广泛应用。如Syskeeper-2000网络安全隔离装置和Netkeeper-2000纵向加密认证网关已经在各大电网得到大规模应用。

2 内部安全防护

2.1 操作系统和应用软件漏洞防护

2.1.1 操作系统漏洞

对于各种漏洞而言,操作系统漏洞的危害程度是最大的。一旦用户主机操作系统的漏洞被利用,攻击者便可以利用操作系统的漏洞访问该主机并进行任意操作。例如,2003年"冲击波"病毒全球爆发,其利用的是系统RPC漏洞,病毒攻击系统时会使RPC服务崩溃,使系统出现重启、无法上网等现象;2004年的"震荡波"病毒,该病毒利用Windows平台的LSASS漏洞进行传播,其可导致系统进程崩溃、出现重启等现象,还会使有关程序出现严重运行错误。如这些漏洞存在于变电站自动化系统中,将严重影响电力系统安全运行。

在近期某电科院对本区域内已经投运变电站综合自动化系统进行的一次安全抽查中,工作人员对漏洞扫描仪发现的操作系统漏洞进行分析,并总结出42条高风险漏洞,其中Unix系统11条,Windows系统31条,可见如果变电站自动化系统全部使用

收稿日期:2010-01-23;修回日期:2010-02-26

Unix 系统将会相对安全,但是由于各种原因,目前电力系统 110 kV 及以下变电站几乎全部使用 Windows 操作系统。

针对已经发现的漏洞,微软公司会在第一时间内发布漏洞补丁并打上补丁,这无疑是解决操作系统漏洞最便捷有效的方法。但要在第一时间内把每个漏洞及时修补好,在实际操作中基本是不可能的,所需要的各种资源也是企业无法承受的,况且,新补丁是否和原有的应用系统冲突,这也是需要验证的,即使不冲突但可能需要系统停止服务来进行补丁升级,这些都制约工作开展。因此,需通过对漏洞进行分析并归,有区别对待,针对不同漏洞采取不同的处理办法。

通过对 31 个 Windows 系统漏洞的分析,发现其中 16 个漏洞是由于开放系统 445 端口所引起的,如漏洞插件编号 (Plugin ID)12209,11835,11808,21193,34477 等,其中有 3 个漏洞是由于开放 80 端口引起的,如 Plugin ID 为 25971,28181,11793 的漏洞。Windows 系统自带组件也会因为存在漏洞而成为被攻击对象,如 Plugin ID 为 29314,34413 的漏洞即为“远程 Windows 会受系统消息队列服务(MSMQ)漏洞影响。攻击者可以利用此漏洞在远程主机上使用系统权限执行任意代码。同时发现变电站自动化系统 SCADA 应用软件的支撑软件也存在着漏洞,如 Plugin ID 10673,11214,34398 就分别为数据库软件 SQL,Serve-U 存在的漏洞。

端口 445 提供局域网中文件或打印机共享服务,是基于 Common Internet File System 公共Internet 文件系统(CIFS)协议工作的。端口 80 是为超文本传输协议(HTTP)开放的,这是上网使用最多的协议,主要用于在 WWW 服务上传输信息的协议。

对于上述由于开放端口 80,445 所引起的漏洞,可以检查变电站监控系统是否真正需要该端口提供的服务,如确实不需要则可以将其关闭,或者启用 TCP/IP 筛选,使用 Interne 协议安全(Ipsec)对端口进行筛选,对端口进行定制。对于 Windows 组件,可以根据“最少的服务 + 最小的权限 = 最大的安全”原则,仅仅安装确实需要的服务。对于经分析确认需要安装 Windows 发布系统补丁的情况,在安装前需认真分析该补丁对操作系统及应用软件的影响,安装之前要在模拟的环境中进行先导测试,确认成功之后才能进行漏洞修补工作,实施前做好应用软件的备份等工作。

综上所述,对系统漏洞进行分类处理将使该项工作更有针对性且更加切实可行。

2.1.2 应用软件漏洞

作为应用软件的开发者,各电力自动化厂家应当对所开发的软件负责,采用更加严格的软件安全测试技术,在生产环节就要降低软件存在漏洞的可能性。厂家还应该具备及时提供修补软件漏洞补丁的能力。同时相关管理部门应当建立软件漏洞检测与公告机制。通过软件漏洞检测,尽可能主动挖掘软件的潜在漏洞,并通知自动化厂家发布升级补丁修补漏洞或者推出新版本。

2.2 主机及应用安全

2.2.1 用户名和口令

要运行变电站监控系统首先必须登录操作系统和 SCADA 应用软件,登录则需提供用户名和口令。实际运行中,由于对系统安全不够重视或处于运行维护人员便于记忆等原因,目前运行的变电站监控系统大多数存在着登录操作系统和维护运行监控系统的用户名和口令过于简单的问题,甚至有使用空口令的现象存在,这为入侵者侵入自动化系统运行恶意代码提供了方便之门,对监控系统的安全稳定运行构成重大威胁。针对此类现象,首先,各电力企业人员需对此引起足够的重视,改变以往设不设密码一个样,密码简单复杂一个样的观念;其次,也可以通过技术手段对此进行一些限制,做到防患于未然,为管理员(Administrator)及运行维护人员账号指定安全的口令,保证口令具有一定的复杂度,如需超过 10 位,且由字母、数字和字符构成,把 Administrator 账号重新命名,并且可创建一个陷阱户,如 Windows 系统默认管理员账号 Administrator,该账号通常成为攻击者猜测口令攻击的对象。为了降低这种威胁,可以将账号 Administrator 重新命名,再创建一个名为“Administrator”的本地用户,把它的权限设置成最低,并且加上一个超过 10 位的超级复杂密码,让入侵者误认为这是管理员账户,这就创建了一个陷阱用户;除此之外,还可以禁用或删除不必要的账号,禁用所有非活动账户,特别是 Guest,删除或者禁用不再需要的账户、禁用远程桌面功能、禁用空用户连接,Windows 的默认安装允许任何用户通过空连接得到系统所有账号、共享列表,这本来是为了方便局域网用户共享文件的,但是一个远程用户也可以得到你的用户列表并使用暴力法破解用户密码;激活 Windows 系统的安全策略,Windows 设计的目标就是系统的安全与稳定,为了实现这一目标,通过 Windows 系统的安全策略就可以方便地配置本地计算机的安全设置。这些设置包括密码策略、账户锁定策略、审核策略以及其他安全选项。通过在密码策略中进行设置,增加密码复杂度,提高暴力破解的难度,增强安全性。还需要制定账户锁定策略,如设置

账户登录次数和登录不成功后锁定时间,使得用字典文件的穷举法执行不了。对于 SCADA 应用软件,需要软件提供商也采取同样方法限制非法登录及非法操作,保障自动化系统的安全。

2.2.2 安全审计功能

加强安全审计功能,激活 Windws 安全审计功能,从而从日志中了解到机器是否在被人攻击及非法文件访问等等。SCADA 应用软件也应记录所有与应用相关的操作记录(包括时间、地方、内容、用户行为等)、系统资源(CPU、内存、存储设备)的异常使用也应当记录,当发现异常时需及时报警。

2.3 计算机外部接口管理

2.3.1 杀毒软件

变电站二次系统最直接最现实的网络安全问题莫过于病毒,特别是蠕虫病毒。蠕虫病毒的爆发不仅会导致工作站或服务器系统无法正常工作,还会造成网络系统的瘫痪,导致系统停运,引发电力安全事故。防范计算机病毒最有效的方法莫过于安装杀毒软件,变电站自动化系统也不例外。但由于计算机病毒层出不穷,杀毒软件病毒库也需随之更新,而变电站自动化系统处于一个与外界隔离的网络,杀毒软件不可能做到实时更新,其杀毒防毒功能大打折扣。或者可以采取离线升级病毒库的方式,但此工作量是电力企业所不能承受的,况且杀毒软件和 SCADA 应用软件的兼容性无法保证,以前出现过著名杀毒软件将系统正常文件当病毒误杀导致系统崩溃的事件。可见,在变电站自动化系统中安装杀毒软件并非是有效办法。

2.3.2 移动存储设备的管理

在变电站自动化系统中,病毒传播的主要途径为移动存储设备,如通过移动硬盘、U 盘、光盘等进行传播。还发现在变电站调试过程中存在施工单位人员会借用监控机处理实验数据,或投运后运行人员在监控系统上处理工作文档等行为,而此时绝大多数时候移动存储设备被接入监控机,此时病毒有可能在不知情的情况下被引人自动化系统,为自动化系统安全稳定运行埋下安全隐患。因此,必须强化计算机外部接口管理,电力部门应当制定严格规章制度,专机专用,禁止在变电站自动化系统上进行与运行维护系统无关的工作,禁止在自动化系统计算机上使用移动存储设备,包括光盘等。目前 U 盘病毒最普遍的传播方式是通过 Autorun.inf 文件进行传播的。

因此在监控系统中可以禁用 U 盘的自动播放功能,例如可以关闭 “Shell Hardware Detection”服务,关闭这个服务后再放入光盘或 U 盘时系统将不再扫描这些移动介质的内容,也就不会运行 Autorun.inf 中所配置的文件,或者在 Windows 组策略的控制窗口关闭的自动播放功能等。针对不仅限于在 U 盘根目录下生成一个 Autorun.inf 的引导文件的病毒,可以通过组策略达到禁用 USB 移动存储设备的方法,通过该方法可以做到移动存储设备不能在计算机上使用,而对采用 USB 接口的鼠标和键盘的使用不产生影响。对于光驱设备,一般在自动化系统出厂后基本都不再需要,因此可以建议厂家在设备出厂前将计算机的光驱电源或数据线拔掉,从硬件上阻止病毒通过光盘传播。

3 结束语

电力二次系统安全防护过程是长期的动态过程。变电站自动化系统的安全对电网安全稳定运行起着举足轻重的作用,既要严格按照电监会的要求落实电力系统二次防护的总体原则,同时也应重视各细节部分;既要加强电力企业人员的信息安全观念,又要运用各种合理技术手段不断巩固变电站自动化系统的安全。

参考文献:

[1] 电力二次系统防护规定[S]. 国家电力监管委员会.

[2] 李 劲. 电力生产控制区业务系统漏洞修补研究[J]. 广西电力,2009,32(4):1-4.

[3] 赵 鑫. 漏洞攻击防范技术与漏洞数据库设计[D]. 北京邮电大学硕士研究生学位论文,2008.

[4] 陈 波. 计算机系统安全原理与技术[M]. 北京:机械工业出版社,2006.

作者简介:

魏世贵(1983-),男,四川仁寿人,工程师,主要从事变电站自动化系统应用软件研究工作;

陈朝恒(1975-),男,重庆丰都人,工程师,主要从事变电站自动化系统应用软件研究工作。

Discussion on the Security of the Substation Automation System

WEI Shi-gui, CHEN Chao-heng

(Nanjing Sino-German Protection & Substation Control Systems Co. Ltd., NARI, Nanjing 210061, China)

Abstract: The information security problems of the current substation automation system are analyzed. In order to guarantee the substation systems safety and stability, this paper proposes the method that combines the border and inside protection, hardware and software protections, and the measures are also put forward.

Key words: substation automation system; information security; protection