

针对高危人群的信息安全防护方案初探

王 磊, 夏元轶

(国网江苏省电力公司信息通信分公司, 江苏 南京 210009)

摘 要:近年来, 电网企业信息安全工作的重要性日益提升。从人员角度对信息安全进行分析, 是区别于从设备和系统角度进行分析的新分析方法。从相关人员中甄别出高危人群, 针对其身份特点和行为特征定位出安全事件发生的主要环节, 从此入手对技术和非技术因素进行研究和强化, 提出了针对高危人群同时适用于一般人群的信息安全防护方案。

关键词:信息安全; 防护策略; 高危人群; 电网企业

1 研究背景与研究内容

1.1 研究背景

近年来, 随着信息安全工作重要性的不断凸显, 作为国民经济重要支柱行业的电力行业, 其信息安全工作在保障企业安全生产和支撑企业正常运转的基础性作用不断提升。

其变化体现以下方面: 首先行业主管部门的监管工作不断加强。国务院国资委、国家能源局(原电监会)、国家保密局、国家密码管理局等主管部门每年均对重要信息系统安全等级保护工作、商用密码安全工作、信息安全保密工作进行工作部署和多次监管检查。其次总部管控力度日益严密。总部制定了电力二次系统“安全分区、网络专用、横向隔离、纵向认证”、管理信息系统“双网双机、分区分域、等级防护、多层防御”的整体策略, 并每年定期开展信息安全治理工作。第三, 社会公众及第三方组织重点关注。以乌云网站为代表的位于厂商和安全研究者之间的第三方安全平台近年来对电力行业尤其是电网企业的信息安全工作十分重视, 多次公布电网企业信息系统漏洞。

在此背景下, 电网企业的信息安全工作愈加重要, 但由于历史和现实的原因, 信息安全工作仍存在诸多不足, 一是尚未全面建立信息安全主动防御体系。近几年来, 在总部的领导下已经初步建立了全面、完善的防护体系, 但对于信息安全出现的新问题、新趋势, 依靠现有的被动式防护体系仍存在较大不足。二是公司系统负责数万名员工终端、数十万电网终端设备及数十个重要信息系统的安全工作, 工作量巨大, 人员配置仍然较为薄弱。

1.2 研究内容与研究视角

本文以信息安全防护策略为研究内容, 提出满足企业实际情况且便于实施的信息安全防护方法, 确定安全防护工具, 在此基础上确定安全防护方案。

本文采用的研究视角不同于以往从设备、系统角度分析, 而是从参与信息工作的特定人群——信息安全高危人群的角度进行分析与研究, 从而将常见的技术视角扩充为包含技术和非技术因素的更加广泛的视角进行分析。

将参与信息工作的人当成将信息安全工作的研究对象, 从其身份特点和行为特征进行分析, 是对信息安全研究工作的新尝试, 具有一定的实践意义。同时电力行业属于国家安全和国民经济命脉的重要行业和关键领域, 对其员工及其信息安全关联方应比照政府机关人员信息安全考核机制^[1]执行。

2 高危人群与危险点分析

2.1 高危人群分析

高危人群(high risk group)是指一些具有某种危险性高的特征(多指疾病)的人群组合。在信息安全工作中引入“高危人群”的概念, 有利于梳理出信息安全薄弱环节和危险源, 便于采用具体问题具体分析, 因材施教“防”的防护指导思想。

经过近年来的信息安全工作实践, 我们认为, 信息安全工作也符合“二八定律”, 即 80%的信息安全事件与 20%的人员有关, 这类人员一般为外来人员、借调人员(含长期出差人员)、试用期人员和基层农电员工, 本文所指的信息安全高危人群主要指上述四类人员, 其身份特点和行为特征的分析如表

1。

表1 信息安全高危人群分析表

| 人群名称 | 身份特点 | 行为特征 |
|--------|---------------|---------------|
| 外来人员 | 非组织内部人员 | 流动性强，外部联系多 |
| 借调人员 | 临时短期工作 | 流动性强，人员变动大 |
| 试用期人员 | 新进组织人员 | 不熟悉规章制度 |
| 基层农电员工 | 基层人员，知识技能相对欠缺 | 不熟悉计算机基础知识和技能 |

2.2 危险点分析

当前，电网企业内部存在的安全风险主要包括：人员信息安全意识薄弱、防护措施不及时、操作不当等人为因素、人为的恶意攻击和泄露、信息存储和传输安全级别低等^[2]。具体的说，目前信息安全的重要考核工作如表2。

表2 信息安全重要考核

| 考核点 | 常见情况 | 高危人群 |
|------------|---------|------------|
| 违规外联 | 3G网卡使用 | 外来人员、试用期人员 |
| | 长期电脑未使用 | 借调人员 |
| | 外部维修 | 基层农电员工 |
| 邮件保密字 | 外发邮件 | 试用期人员、外来人员 |
| 内网数据流失 | 非安全U盘使用 | 试用期人员、外来人员 |
| 非内网计算机接入内网 | 外来笔记本接入 | 外来人员 |

3 安全防护方案

3.1 技术部分

针对当前电网企业信息安全现状^[3]，拟从内网安全管理、互联网安全管理和存储与桌面安全管理三方面进行技术安全防护。

内网安全管理是指在电网企业内部网络特指信息大区上采用的技术手段和工具，主要包括：主机登录控制、网络访问控制、磁盘安全认证、磁盘读写控制和内网主机全程追踪审计^[4]。其逻辑过程如图1所示。

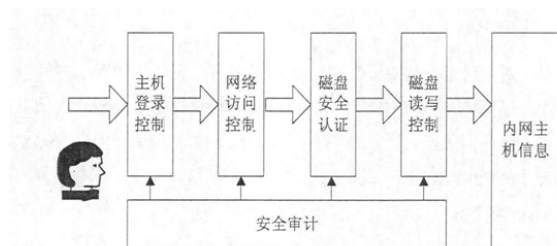


图1 内网安全管理逻辑图

通过上述内网安全管控手段，非授权的用户首先无法获取到内网的IP地址，无法使用网络。登录

网络后，除网站等非登录的应用系统，均需要主机登录控制。同时磁盘的安全管理使得内部数据无法复制到外来存储介质上。从登录网络、登录主机到磁盘读写操作，各环节均有安全审计系统、子系统、模块或功能进行监控或纪录，从而全过程可追溯可追究。

互联网安全管理是指在电网企业信息外网上采用的技术手段和工具，主要包括：互联网出口统一管理、互联网出口安全管控、外网服务区与用户区隔离、DMZ区安全加固、无线网络安全应用和移动终端安全接入等。

通过上述互联网安全管控手段，实现了统一的互联网安全管控，从企业内部向互联网看，部署上网行为监控系统、邮件敏感字检测系统，杜绝各类用户从内部向外传递敏感信息。从互联网向其他内部看，在互联网与信息外网部署防火墙、IDS等安全设备。在必须的信息外网和信息内网边界上部署逻辑隔离设备，仅允许部分信息通过隔离设备进行安全穿透。同时严格管控无线组网和企业内部的移动终端。实现了“双网双机、分区分域、等级防护、多层防御”的总体安全要求。

存储及桌面安全管理是指在移动存储和桌面终端的技术手段和工具，主要包括：安全移动存储管理、桌面终端监控程序管理等。

通过上述管理手段，实现了所有内外网注册桌面终端的全面管控，对桌面终端的网络访问信息、涉密文档、系统漏洞均可进行监控。同时桌面终端只允许注册授权的安全移动终端进行数据复制等读写操作，确保了注册桌面终端的数据安全。

综上所述，通过全面的技术防护措施可以对外网、互联网和终端及存储进行较为全面的安全管控，但迷信技术手段，忽视管理是信息安全工作的一个重大误区，非技术部分的安全防护工作是更需要注重的方面。

3.2 非技术部分

非技术因素是信息安全的重要部分，我们认为在信息安全工作方面，技术因素是必须的，非技术因素是更加重要的。传统的安全防护方案侧重于技术层面的防范与管控，但非技术因素方面的制度保证、人员管理和流程管控却成为薄弱环节。

在制度保证方面，建立健全内外网IP地址申请制度、账号开通制度、内外网设备登记制度、安全

存储设备申请制度等一系列安全规章制度。从制度上对外来人员、试用期员工等进行严格控制。

在人员管理方面,坚持全员信息安全培训,发放信息安全手册,将信息安全内容纳入安规考试,全员签订保密协议,从而将包含四类高位人群在内的所有人员进行全面管理。

在流程管理方面,对外来人员进入企业内部工作的,按照工作需求分配计算机终端和安全存储终端,岗位变更和离职等流程严格信息安全管理。对计算机修理流程进行规范,杜绝外部维修队伍对内网计算机进行维修。

综上所述,信息安全防护工作的非技术部分应当常态化、持久化,注重制度建设、强化人员和流程管理,可以以较小的成本实现较大的效益。

4 效果与展望

近年来,国网江苏信通公司在信息安全实践中,借鉴本文的提出的重点防护思路对外来人员、试用期人员、借调人员进行了较好的管理,未发生信息安全事件。同时在对基层单位的业务指导上,也强化了针对高危人群的防护宣贯。往年发生多起的违规外联、非安全 U 盘使用等信息安全事件也逐年下降,取得了较好的成效。

信息安全是信息化建设的永恒主题,只有持续规范安全管控、治理薄弱环节、持之以恒地建设和完善,不断提高管理水平和技术防护水平,才能在安全可靠前提下,并以信息化持续稳定地支撑助力生产专业化与管理现代化。

从人员身份分类和行为特征角度进行的分析是

可以深入开展并富有一定实践指导意思的分析手段,本文仅仅对此进行了初步的尝试。信息网络和信息系统应在此分析工作的基础上,利用此方面的研究成果,增加相关功能,更加智能地判定用户身份,并推导出其行为特征,从而对可能发生的信息安全风险进行主动防御,实现更高层次的信息安全防护,为信息化建设、运维工作打下坚实的安全基础。

参考文献:

- [1] 张嫣玲. 政府机关人员信息安全考核制度初探[J]. 网络安全, 2010(07): 57-59.
- [2] 张昕. A 供电公司信息管理安全与防范对策研究[D]. 兰州: 兰州大学, 2011.12-14.
- [3] 赵婷, 陈雪鸿, 李怡康, 等. 电力信息安全水平评价指标体系构建[A]. 2012 电力通信管理暨智能电网通信技术论坛论文集[C]. 北京: 中国通信学会, 2013.204-205.
- [4] 李金长. 企业内网信息安全防护系统设计与实现[D]. 成都: 电力科技大学, 2010.18-19.

作者简介:

王 磊 (1978-), 男, 江苏扬州人, 高级工程师, 从事信息技术管理工作, E-mail: wang.lei@js.sgcc.com.cn;
夏元轶 (1988-), 男, 江苏无锡人, 助理工程师, 从事信息安全管理, E-mail: xiayuan yi@js.sgcc.com.cn。