油气基础设施、电网成网络攻击“重灾区”,可再生能源电力网络保护措施有待提升——

能源网络安全成全球焦点话题

■ 本报记者 李丽旻

近日,行业分析机构标普全球普氏的“原油安全哨兵”研究项目发布最新报告称,自2017年以来,全球针对能源领域的网络攻击数量激增,其中,油气基础设施、电网两大领域已经成为网络攻击的“重点区域”,在全部网络攻击事件中的占比超过五成。在全球能源转型大潮下,如何维护网络安全已然成为能源领域新的热点话题。

传统能源设施受攻击频次激增

根据“原油安全哨兵”统计的数据,过去5年,在所有网络攻击事件中,针对油气基础设施的占比约为1/3,针对电网的占比约为1/4。其中,偷窃能源相关数据、攻击网络系统致其瘫痪是黑客采取的主要手段,美国、沙特、英国的能源网络遭受攻击最多。

标普全球普氏指出,过去一年里,最受关注的网络攻击事件是美国长达数千公里的Colonial输油管道系统遭袭,导致美国东海岸南至佛罗里达州、北至弗吉尼亚州等多州加油站关停。据美国司法部副部长Lisa Monaco透露,美国政府最终向黑客支付了230万美元。

去年下半年,全球多国的石油基础设施都遭到了网络攻击。比如,去年7月,沙特阿美确认该公司部分数据遭到泄露,并遭遇网络勒索,涉及金额高达5000万美元。而今年2月,德国两家成品油供应商也表示,公司网络遭到黑客袭击,导致当地汽油供应出现中断,并对欧洲多个交通运输枢纽、物流运输造成负面影响。

研究报告同时指出,近年来针对传统能源设施的无人机物理袭击事件数量也有所增加,但从目前的技术水平来看,无人机袭击事件难以找到源头,同时难以防范。

风光发电“数字风险”与日俱增

除传统电厂、油气基础设施外,风力和光伏发电站也成为网络攻击的重点对象。去年11月,欧洲风机制造商维斯塔斯发布公告确认,该公司多个地点的风机遭到网络攻击,部分风机的内部控制系统和数据遭到破坏,该公司不得不大范围关停风机。

油价网援引多位业内专家的话称,不论是光伏逆变器还是风机控制系统,都存在遭受网络攻击的风险。随着各国不断推动能源转型,风力和光伏发电量在能源供给系统中的占比正不断增长,针对可再生能源基础设施的网络攻击也应该引起各界的重视。

网络安全专家James Walsh在接受油价网采访时指出,与传统油气基础设施相比,目前快速发展的可再生能源发电系统与电网连接更加紧密,可能造成的系统风险相对也更高。

“通常情况下,可再生能源发电设施与电网直接相连,同时为了智能化管理,大部分风电、光伏系统都使用了智能系统,数字化程度较高,这为网络攻击提供了温床。可再生能源基础设施面临的‘数字风险’正在加大。”James Walsh表示。

同时,在数字风险管理公司Axio创始人James Walsh看来,一直以来,风电和光伏发电的规模在电力系统中的占比远低于化石燃料发电,这导致各国在一定程度上对可再生能源发电设施的数字安全重视程度不如传统能源。“但是在部分地区,可再生能源发电占比已经超过了1/3,提高可再生能源发电设施的网络安全保护等级势在必行。”

加大投入必不可少

多家外媒指出,一直以来,能源公司对政府提出的网络安全要求往往采取“忽视”的态度,但自美国原油管道遭到网络攻击后,各界明显提高了对关键基础设施数字安全的保护意识。

实际上,据行业媒体Cybersecurity Dive报道,近年来,保险公司对于能源企业面临的潜在数字威胁已经“十分关切”,过去一年里,美国各电力公司的网络安全保险费用上涨了25%-30%,其他能源公司的网络安全商业保险费用也增长了一倍以上。

业界普遍认为,目前,鉴于网络黑客使用的攻击手段十分复杂,可再生能源电站运营商应该在系统设计之初就考虑到网络安全问题。另外,也有专家指出,电站运营商还需提升在遭受攻击后恢复正常运营的能力。

“对已经建成的风光电站网络系统进行更新和加强,并加大对员工的培训力度,都将变得十分重要。”数字技术公司Sentient Digital分析师Matt Donahue表示。