成功案例

[即时发布]

《伦敦陷落》对电网“开挂” 电力行业如何防御黑客攻击？

大唐河南发电有限公司部署亚信安全 树立电力行业工控安全标杆

看过《伦敦陷落》的观众一定感觉“脑洞开的有点大”，但恐怖分子黑客切断全伦敦的电力，确实在全球范围已经出现过类似案例。那么，作为“一定要”重视网络安全的电力行业，又当如何在现实中应对黑客威胁呢？

作为行业中率先部署信息安全解决方案的代表企业，大唐河南发电有限公司（文中简称：河南发电）采用亚信安全威胁发现设备（TDA）与 Web 安全网关（IWSA），全面提升了整网威胁发现能力，进一步提升网络防御能力，为信息安全技术在电力行业的落地踏出了坚实一步。

“十年合作”换来技术信任

电力行业是与生产生活息息相关的基础行业，而自去年乌克兰电网遭受袭击事件之后，国内外都在积极探索、部署和推广相关的信息安全技术。作为省级公司，河南发电不仅在电力能源投资、建设、生产、经营方面，以全资和控股形式管理河南、湖北两省下属 24 家单位，同时还在工业控制安全技术实践和落地推广方面积极探索。

据河南发电相关技术负责人介绍，“从整个行业来看，国际环境和攻击事件的曝光迫使电力行业积极配合安全技术推广，我们更需要将安全做在前面。电力行业早期面对的安全问题主要来自于两方面，不完善的安全制度与不成熟的安全防护技术都亟待完善。因此，河南发电在选择技术合作伙伴和服务商时也十分谨慎。”那么，河南发电与亚信安全的合作又是从何时开始的呢？

“十年之前”的一次大规模安全产品部署，是一次关键性的技术变革。据介绍，在终端安全防护层面，河南发电存在一段杀毒软件使用的“空白期”。在此期间，部署的免费杀毒软件并没有达到“企业级”的要求，其根本原因在于免费软件并不提供后续支付与服务能力，在杀毒效果和病毒侦测率、统一管理等方面很不理想。为此，河南发电与亚信安全（原“趋势科技中国有限公司”）达成了合作，并在 2006 年陆续部署了终端安全产品，其效果和防御能力得到了充分检验，这为双方后续合作奠定了良好基础。

“主动防御”弥补管理短板

多年之前，网络安全软件很难甄别攻击是如何发生，但随着信息安全技术的不断创新，网络攻击正在得到有效地拦截，黑客的进攻路径也可以在最新的安全产品下显露无疑。

追溯过去的安全事件，河南发电下属单位出现过多次网络异常且缓慢的状况，受制于当时技术条件，很难界定是攻击是在内网还是外网，而选择亚信安全的威胁发现设备（TDA）与 Web 安全网关（IWSA）则弥补了这一技术短板。

河南发电相关技术负责人表示：“在内网，以 TDA 为核心的解决方案能够很清晰地发现某一个时间段内的安全威胁，进而追溯威胁来源，对原有的钓鱼网站、木马、窃取数据等行为全面侦测。在边界过滤层面，亚信安全的 IWSA 有着云安全技术提供动态实时分析，在实际使用过程中感受更为直观，为我们拦截了数量庞大的非法攻击。比如，主动拦截了财务部门终端应用的恶意插件，发现恶意木马在内网的横向扫描，等等。”

当然，一款让用户满意的安全产品肯定与配套服务体系是分不开的。据介绍，在产品部署与使用过程中，河南发电就遇到技术支持和应急响应的情况，而亚信安全技术支持团队也用高效的服务和过人的技术充分证明了这一点。

信息安全管理进入“新常态”

亚信安全的 TDA 与 IWSA 满足了河南发电对信息安全管理的刚需，从功能特点到后期技术支持，再到云安全智能防御网络的主要预警，这些都能够满足安全策略主动化、统一化的需求。在充分验证之后，河南发电将以统一安全标准的方式，要求下属单位尽快部署安全防护解决方案，进一步推动信息安全技术在公司内部的落地实施。

另一方面，对于传统网络安全软件而言，工业领域安全还是存在许多技术盲点，河南发电与亚信安全也正在联手寻求这些问题的答案。据悉，河南发电已经考虑部署亚信安全的移动办公与虚拟化安全防护解决方案，从网络、终端、云端形成更加完备和智能的防御体系。

##

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式 ,助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。更多关于亚信安全公司及最新产品信息，请访问: http://www.asiainfo-sec.com