

网络安全

网络威胁的目的

对电力行业运行，以及人们日常生活离不开的可靠电力供应的威胁，已经不仅仅停留在理论方面了。在过去 4 年所报告的工业控制系统事件中，大约 250% 的突然增长证明了仅仅依靠调控无法保护电力基础设施，这个行业每个人都需要提高有关意识和技能。

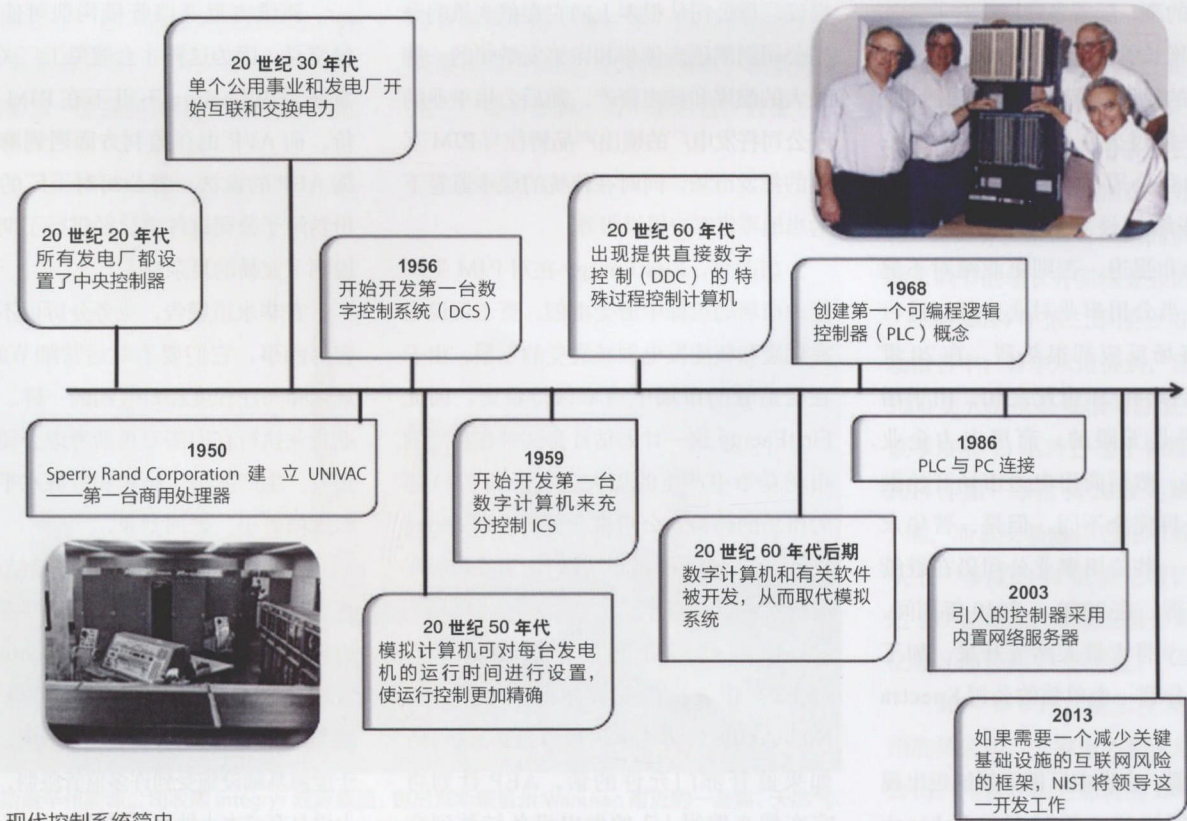
文 | Michael Assante

作为一个资深网络安全专家，有必要观察行业内部在网络安全和技术进步方面对话的进展。网络安全第一次成为全球对话的一个主流话题，这可能是当前最重要的一件事。

网络安全领域的实践，保护个人、企业或政府网络和计算机的业务已经开

展了 30 多年，但此前两年发生的事件使人们的注意力很快聚焦在不断增长领域中的挑战和问题。鉴于过去的对话仅仅关注需要适当的网络安全水平来保护联网系统，今天的企业在问：是否存在一个能保护企业免受目标攻击的网络安全模型？答案是“存在”，但是保护措施

的执行却是复杂的。必须注意到，企业领导者开始理解直接面向消费者的企业正受到越来越多的共同攻击，以及这些攻击与具有更大潜在破坏力的工业系统和关键基础设施攻击的关系。本文对近年来网络攻击的频率和步骤进行了分析，以保护电力行业运行技术。



现代控制系统简史

公众意识正在提高

关于人们怎样认识网络安全这个问题，没有比索尼电影公司前几年受到的攻击更好的例子了。在这个案例中，敏感邮件、员工社会安全号和私人医疗信息被人泄露出去，使全球任何一个网民都能看到。这些美国政府认为与朝鲜有联系的攻击者，甚至窃取索尼电影公司的影片，例如《狂怒》和《安妮·纽约情缘》的重拍版，来破坏影片以不同形式进入市场的商业模式。

JPMorgan Chase、Target 和 Home Depot 这些大公司作为受害者对超过 16 个月的网络攻击进行了有力打击，而对索尼电影公司的攻击才是提高公众的网络安全意识的最重要因素。根据《SC Magazine》最近的一篇报道，预计超过 5600 万信用卡和借记卡与 5300 万张个人邮件地址信息在 2014 年 4 月对 Home Depot 的网络攻击中被窃取。摩根大通银行此前 3 个月被黑，使全球超过 7500 万家庭受到影响。

必须认识到针对 Home Depot、Target、JPMorgan Chase 和成千上万大公司的互联网犯罪的首要动机是高度破坏来获得经济上的利益。但是，这些攻击也带来一些意想不到的后果，例如唤起公众对网络安全的意识，至少是对互联网沟通中的漏洞的意识。

在 2014 年 12 月，一家全球安全服务和产品公司 Cylance 对他们为期两年的网络攻击调查行动发布了一份报告。这篇名为《手术刀》的报告引用了大量的证据，伊朗已经开始了一项可持续活动来控制敏感计算机网络，包括军事机构、国防设施、一般航空设施、石油和天然气公司，当然还有电力设施。

与攻击一家公司差不多，成功地侵入关键基础设施网络也能使每个人受到严重伤害。众所周知，公用事业保存着大量客户信息，可以说比其他零售和服务公司都要多。其他的相同点就没有了，与攻击保存大量账户信息的系统不同，如果攻击者成功地渗透关键基础设施，他们的主

要动机可能不是经济方面的，这种攻击的目的更有可能是通过妨碍公共安全和生产力来威胁使一个国家运转的基础系统中断运营。希望侵入一个国家的基础设施或通过摧毁价值观来破坏经济的攻击者已经决定要冒着引起有关反应的风险。

威胁随着网络互联性的发展而演变

电力行业就像世界其他地方一样，由于数字互联而日益扩大。过去的操作技术 (OT)，例如工业控制系统 (ICS)，都是独立、未联网的。近年来，数据驱动分析应用软件和跨平台通信等技术已经引入工业系统，以提高生产力和可靠性水平。而且达到了目的，尽管原有系统并不是为了和这种技术进行整合而设计。

现代自动和控制系统目前与企业网络和外部网络连接，使运营商和供应商能远程控制、监测和维护操作的每个方面，最终改善生产率、提高性能和节约成本。通信技术还用于接入一个扩展后的全国供应链，使制造业和基础设施运行更紧密地追随全球市场。在这些先进技术提高效率时，它们还会带来新的攻击面和一些复杂问题，暴露一些漏洞，使攻击者有机可乘。在采用联网数字系统前，对手需要进入实际现场来危害控制系统或派人亲自攻击生产系统。互联系统和远程接入技术的推出使一些怀有恶意的人能从世界任何地方侵入生产网络。

OT 的数字先进性使电业行业的发电、运输和供电更加高效。但是，破坏性的网络攻击会影响安全可靠操作的核心能力。对这些系统的威胁减少了可预见性，提高了人们的安全意识。对工业系统成功的攻击不仅会影响控制系统，而且攻击者还可以直接影响流程，并恶意操作受到控制的设备，带来安全问题。

对关键基础设施 OT 的威胁不再只停留在理论上，攻击者们正在潜心研究这些设施的漏洞。通过互联网侵入连接电网 OT 系统的网站就能收集信息、认证证书、发现进入负责发电和供电安全可靠

性的系统的路径。许多政策制定者认为，美国经历一次会导致严重后果的攻击只不过是时间问题。

行业或关键基础设施的网络攻击已经从地下转到地上。一家德国联邦机构报道说，2014 年下半年，一家钢铁企业的运行受到网络攻击，导致炼钢炉受到物理破坏。攻击者声称通过一封恶意邮件进入这家钢铁企业的系统，从而破坏工厂的控制系统和进行物理破坏。虽然网络攻击很难对一家工厂进行破坏，但是我们已经看到 ISC 攻击的发展。

在过去几年，由于技术漏洞和人力失误导致许多针对电力和公用事业公司的威胁。但今天的威胁已然不同，这些威胁更有针对性。对 ICS 攻击的动机不同，它们都能侵入、研究和控制运行，从而带来更大范围的破坏，远远超出基础设施运营商。

电力行业需要更好的培训

互联网正在变得更有针对性与破坏力，关键基础设施的工作人员在解决这种威胁方面都缺少培训。根据 SANS 研究所的说法，电力行业约 1 万名从业者需要接受如何防御网络攻击的培训。这些攻击都是很复杂的，漏洞总是能被发现，所以控制系统工程师必须与网络安全专家进行网络威胁探测、减少和响应方面的交叉培训。

电力公司需要创建一个全面的安全策略来适应我们生活的互联世界。战略不仅要解决物理安全问题，还要建立网络的周边环境。在考虑有针对性的网络攻击时，总是要假定攻击者利用连接到互联网或者一个可访问无线信号的任何很难发现的设备或网络。系统的互连性和新数字组件的引入共同促进网络攻击面的产生，而系统设计、网络安全策略和计划必须将其考虑在内。

我们面临的共同挑战是开发安全功能，推动他们深入我们的设施和生产系统。如果一个公司想要获得数字技术带来的好处，它必须确保系统运作良好、保持完整性。[MM]