

威努特：构建工控系统威胁预警和安全态势感知能力

撰文 / 赵龙

随着工业化和信息化的深度融合，装备和工厂实现互联互通，工业控制系统越来越多地采用信息技术和通信网络技术，逐渐成为工业互联网的一部分。但是，随着大量关键信息基础设施接入互联网，工业互联网安全状况正日益引起人们的担忧。智能设备作为网络的接入点，随时暴露在网络攻击之下。全球工业互联网的安全现状并不乐观，公开的工

业控制系统漏洞数量逐年递增。截止今年9月份，国家信息安全漏洞共享平台（CNVD）收录的工控漏洞数量已经达到1264个，公开的安全事件数量多年来一直居高不下。

2012年美国国土安全部通过Project Shine项目搜索暴露在互联网上的关键信息基础设施，收集了全球范围内超过220万条数据，并确定其中7200个为美国关键信息基础设施。



11月7日，第十九届中国国际工业博览会开幕。国内专业工控安全解决方案提供商北京威努特技术有限公司在会场发布“工业互联网雷达平台”和“工控系统行业漏洞库平台”两款新产品。

“工业互联网雷达平台”是为智能制造企业和政府监管部门等单位提供工业互联网资产探测、漏洞预警与宏观安全态势展现等服务的平台化产品。该平台支持 Siemens S7、Modbus、IEC 60870-5-104 以及 DNP3 等 38 种以上的工控协议指纹识别，支持工控设备无损漏洞探测，实现全球工控设备信息和漏洞信息的隐匿探测及全局采集，同时准确定位工控设备。

“工控系统行业漏洞库平台”汇总 CVE、NVD、CNVD 和 CNNVD 等多个漏洞库的数据，提供“漏洞检索”、“漏洞统计”和“漏洞月报”等功能，收集工控漏洞解决方案和补丁信息，实现与监管部门、关键信息基础设施运营者以及有关研究机构、网络安全服务机构间的网络安全信息共享，帮助用户自我发现并解决工控系统的安全风险。

今年 10 月，美国国土安全部与美国联邦调查局 (FBI) 发出联合声明，证实制造商的工业控制系统遭受黑客攻击的案例已经扩大至能源、核能与供水等公用事业单位。

工业控制系统信息安全简称工控安全，是对关键信息基础设施上信息安全和防护的响应，属于工业互联网安全的一部分。对关键信息基础设施的安全风险进行有效检测评估、掌握全网信息安全态势以及实现网络安全信息共享，符合国家安全战略，在《网络安全法》中有明确要求。

威努特行业解决方案技术总监姜立群表示，我国工控网络安全监测预警和应急响应问题长期得不到解决。过去几十年我国建设了大量关键基础设施、重大工业控制系统，大部分是依靠国外厂商的设备和技术建立起来的。控制设备普遍存在的已知漏洞、未知漏洞以及可能存在后门，成为阻碍我国制造业快速发展的绊脚石，也是国家安全的重大隐患。通过“工业互联网雷达平台”和“工控系统行业漏洞库平台”，企业可以掌握自身工控资产网络暴露情况，感知工控网络威胁态势；监管机构可以实时了解接入互联网的工控设备数量及地理位置分布，掌握重要工控漏洞的影响态势，进行工控网络安全监测预警和应急响应。

发布会后，姜立群接受本刊采访。

智能制造：一些企业的业务部门对工业网络安全威胁缺乏充分认识，您对企业工控安全建设有哪些建议？威努特能为企业提供怎样的帮助？

姜立群：工业控制系统的网络安全由于是保障性的，并不像建设业务系统那样立竿见影，因此没有得到一些企业充分重视。像电力、石油石化、轨道交通和智能制造等很多行业的工业控制系统，都属于国家关键信息基础设施，2017 年 6 月 1 日正式实行的国家《网络安全法》，对其信息安全是有明确要求的；2017 年 7 月 1 日起施行的工信部《工业控制系统信息安全事件应急管理工作指南》，对工控系统安全监测预警、应急响应都有了详细规定。落实法规政策，将是这些企业接下来的一项重要工作。

但是，工业控制系统的网络安全建设也不可能一蹴而就，如果选择的方案和产品与业务系统兼容性不够，没有经过充分的验证性测试，将对业务系统的正常运行产生不可控的后果。所以，我建议企业在考虑工控安全建设时，按如下步骤进行。

先做安全自查，使用我们本次发布的两款平台产品，通过“工业互联网雷达平台”自我检查企业工业控制系统有无暴露在互联网上的设备，通过“工控系统行业漏洞库平台”查找使用的设备型号有无已知漏洞存在，来对企业自身安全状况有个初步认识。

再做安全服务，包括安全培训、现状调研、风险评估以及安全测评等服务，增强人员的安全意识，了解国家政策法规对本行业工控安全的要求；摸清本企业工控系统的安全现状，以及与政策法规要求的差距，为后续网络安全建设提供现实依据。

最后做安全建设和实施，根据前期调研和评估的情况，选择适用于本企业的网络安全解决方案，选择经本企业工控系统或类似工控系统验证过的网络安全产品，并选择专业的实施团队进行部署实施，以保障网络安全建设在保护工控系统的同时，不会对业务系统产生影响。

我们威努特除了本次发布的两款平台可用于企业安全自查外，还能够提供专业的安全服务，包括安全培训、安全调查、风险评估、安全渗透、安全测评和安全体系规划设计，协助企业遵守法律规定要求，做好网络安全顶层规划和设计，为后续技术改造提供理论基础。

威努特还提供与业务系统深度融合的技术方案。我们对很多行业的业务流程和网络结构进行深入研究，基于不同行业的业务模型设计网络安全方案，并且已经在很多行业部署实施，在全国有上百家案例，产品已经在电力、石油、石化、燃气以及轨道交通等多个行业广泛应用。

智能制造：目前工业网络安全解决方案实施过程中主要存在哪些难点？

姜立群：谈到工控网络安全解决方案实施过程中的难点，首先我们要明白工业网络的要求和办公信息网络的要求是不同的。

工业网络对可用性要求高，传统信息安全要实现三个目标，即保密性、完整性和可用性，通常都将保密性放在首位考虑的，而工业网络安全的目标顺序正好相反，工业网络安全首要考虑的是所有系统部件的可用性，然后再考虑完整性和保密性。所以传统信息安全的技术可借鉴，但不能直接使用。

工业网络对实时性要求高，控制系统要求响应时间大多在几十毫秒以内，而办公信息系统的实时性可接受秒级的响

应。所以在选择工业网络安全方案和产品时，需要充分评估安全方案对业务实时性的影响，严格选择实时性较好的安全产品，导致可选择的方案和产品较少。

工业网络的个性化定制多，工业控制系统有很多行业属性，不同行业有不同行业的业务场景、应用协议和软硬件架构。所以每个行业在网络安全建设时，常常面临着无产品可选，无方案可用的尴尬情况，需要与安全厂商深度合作开发才能找到真正适合自己业务场景的安全方案和产品。

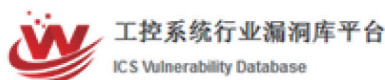
工业互联网建设最大的瓶颈就是安全问题，安全问题不解决，企业很难将工业网络互联互通，很难将生产数据共享汇集，很难将业务流程智能优化。要建设工业互联网，首先得打消业务部门对安全的顾虑，找出不影响业务的安全解决方案。另外，解决工业互联网智能和安全的融合，也是企业深入实施的一个难点。企业的智能化和网络安全系统往往是各自发展的两条线，彼此之间没有包容。比如智能机床，计算资源本来就紧张，如何在不影响性能的情况下解决安全问题？威努特在这方面已经做出了巨大突破，和智能云科合作，面对极大的困难考验，成功把安全融入到智能机床设备，为行业做出了从0到1的示范。

智能制造：企业在筹划工业网络安全方案时，除了选择常规的安全产品和技术，还有哪些更先进的产品和技术可以

考虑？

姜立群：目前很多企业做网络安全方案时，考虑更多的是合规要求，选择工业防火墙、监测审计、主机防护等常规类安全产品进行方案部署和实施，研究型 and 态势感知类产品目前较少选择。工业控制系统一般都属于关键信息基础设施范围，网络安全法对关键信息基础设施要求在网络安全等级保护制度的基础上，实行重点保护，所以企业还应该考虑如何实行重点保护。前面提到的《工业控制系统信息安全事件应急管理工作指南》中，对工控安全应急技术机构有明确要求，负责工控安全风险监测、态势研判、威胁预警、事件处置等工作，这个要求对其他规模较大、技术实力较强的工业企业也有较强的借鉴意义。我的意见，企业在选择常规安全产品和技术以外，应该逐步选择一些监测预警、态势研判类产品和技术，使自己逐步具备较强的安全事件应急处理能力。

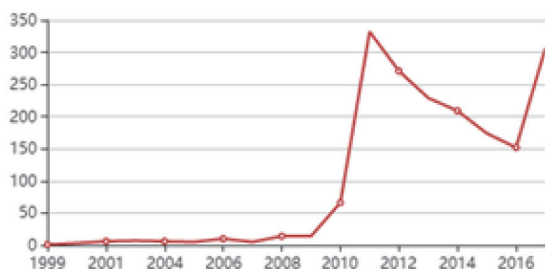
此次工博会威努特发布了两款引领工控安全新方向的平台类产品就是此种类型，一个是工业互联网雷达平台，另一个是工控系统行业漏洞库平台。工业互联网雷达平台主要用于探测暴露在互联网上的工业控制设备、工业系统的工作站和服务器、组建工业网络的网络设备，并深入探测这些设备的漏洞情况，提供基于地理区域、工控设备类型、工控协议等多维度进行态势分析，提供企业版用于企业自身内部部署。工控系统行业漏洞库平台用于收集、整理和分析工控系统的



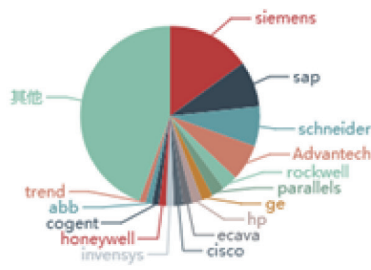
首页 漏洞检索 漏洞统计 漏洞月报

漏洞统计 获取最新漏洞统计信息

工控漏洞趋势



工控漏洞厂商分布



漏洞信息。目前该平台是国内工控漏洞最全面的平台，为关注工控的用户提供详实的漏洞数据和分析数据。

智能制造：威努特工业网络安全产品和技术目前的市场情况如何？具有哪些优势？

姜立群：近年来威努特一直在工控安全领域深耕细作，获得多个政府部门和众多客户的高度认可。是国家工控安全实验室理事单位，工控安全相关国家标准制定的重要参与者和推动者。被公安部授予工控安全技术支撑单位，参与了2016年全国网络安全大检查，受邀保障杭州“G20峰会”、“一带一路”国际合作高峰论坛和十九大。威努特在国内首家提出工业网络安全“白环境”解决方案，迄今已有百余家成功案例，落地项目及市场占有率在国内遥遥领先。

威努特的优势有以下几点：一是解决方案覆盖全，拥有电力、石油、石化、市政、烟草、化工、军工、轨道交通等十几个主流行业的定制化解决方案；二是团队技术实力强，拥有一支由资深安全专家、自动化专家、高级产品研发工程师、优秀企业管理人才组成的专业化团队；三是专注，自成立以来，一直坚持在工控安全领域深耕细作，坚持主航道不动摇，有战略定力，做到专注专业专心，也成功收获了客户的赞誉和认可。

智能制造：您认为工业网络安全的发展态势和未来技术趋势是什么？

姜立群：工业网络的发展，会逐渐打破传统各个工业企业的信息孤岛状态，工业互联网时代，会极大的缩短最终消费者需求和产品开发间的距离。工业网络安全的发展，从应用场景角度分析，应该是以控制系统的核心安全为基础，向业务系统整体安全发展，再到整个工业互联网安全的趋势。目前做工业网络安全大多数方案还局限于保护整个工业流程里面的一个环节、一个子系统的安全，对于不同业务系统对接考虑较少，对于互联网接入环节考虑的更少；未来随着工业互联网技术发展，在保护基于底层关键控制系统基础上，会结合业务全流程模型，构建业务系统整体安全防护体系，即由工控网络向工业互联网转变。

未来的技术趋势，应该是在当前常规安全防护产品和技术的基础上，向工控威胁情报收集和态势感知的方向发展。常规安全产品是躯干和四肢，是执行单元；而威胁情

报和态势分析是神经和大脑，是决策单元。威努特正在做这方面的技术研发，本次工博会发布的这两个平台产品就是在扫描互联网上的安全态势，为常规安全产品的策略部署提供决策依据。

后记：

安全是发展的前提和保障。安全的工业互联网平台对于促进“互联网+先进制造业”的发展具有重要的作用。10月30日，国务院常务会审议通过《深化“互联网+先进制造业”发展工业互联网的指导意见》。安全保障方面，重点加强工业互联网安全技术手段建设，形成国家、行业、企业协调联动的工业互联网安全工作格局，建设覆盖产业全生命周期的安全保障体系。IM