工业技术 3 卷 2 期
ISSN:2661-3662(Print); 2661-3654(Online)

探析网络技术背景下的工业网络安全防护

刘　新

湖南省中标项目投资管理有限公司　湖南　长沙　410000

摘　要：在时代变化科学技术创新过程中，网络技术已经成为各个行业的核心部分，对工业领域而言，网络技术的应用不仅可以控制生产过程中投入的成本同时能够获取更多实质性利益，但在发展过程中如何确保工业网络已经成为目前急需解决的问题。在文章中，基于网络背景下，对工业网络安全防护进行分析和研究。

关键词：网络技术；工业网络；安全防护

引言

随着现代信息网络技术的进步和发展，网络的传输安全性与稳定性成为当前的主要研究话题，尤其在工业中，实现网络协议与以太网协议的结合，不仅能够满足当前的网络稳定性发展要求，还能促进网络设备性能的提升。随着信息网络技术的发展，网络传输速率、稳定性、可靠性等有了很大的进步，技术的进步促进了以太网络向工业网络的延伸。工业网的应用是对传统以太网络技术的延伸，是工业网络协议和以太网络协议的结合。

一、网络技术背景下工业影响网络安全的因素

1.1 工业网络逐渐开放

传统网络在设计过程中首先考虑的是网络本身具有的开放性性，因网络终端数量越来越多且功能不一，故而许多不法分子借助其中存在的漏洞谋取私利，这一点同样存在与工业网络中，犯罪分子主要目的是通过入侵网络盗取具有价值的信息或破坏某些实体设施。此外因工业网络以传统网络为基础，故而传统网络中存在的漏洞同样可能出现在工业网络中，导致系统防御力降低，网络和设备安全性无法得到保障，工业设施经常受到网络攻击，以往采取的安全防护措施在运用过程中无法起到良好的实用效果，由此可见工业网络安全防护措施需要不断改进。

1.2 工业设施操作不当

随着计算机使用效果愈发显著，不同企业之间建立了工业网络从而实现资源共享，但是并非所有工作人员都能够正确运用工业网络。因使用者越多工业网络安全性逐渐降低，究其原因发现导致这种情况出现主要是由于员工个人习惯不同，操作过程中可能会出现一些错误操作。譬如员工在工业网络中登录个人账号时如果默认记住密码，不仅个人信息可能会外泄，甚至与工作有关的数据资料也会暴露。

1.3 互联网直接攻击

互联网攻击已经成为影响工业网络安全性的主要因素，一般情况下，可以根据目的将黑客攻击分为主动攻击与被动攻击，主动性的恶意攻击除了会影响工业网络信息的完整性与有效性外，还会影响工业实体的实际操作，而被动性的黑客攻击只会对网络信息的完整性及有效性造成影响，并不会影响到工业实体的实际运作，因此，主动性的恶意攻击对工业网络信息所造成的安全威胁要更严重一些，因此工业企业尽管在升级转型的过程中需要以更为开放的态度去运用新技术，但前提是在充分保障自身信息安全的基础上进行。

1.4 工业内网病毒攻击

工业网络病毒主要来自于互联网，病毒会根据事先编制的程序选择目标具有定向特征，因此在传播过程中并不具有较强的攻击性。当病毒入侵之工业网络当中，会自动寻找攻击目标，从而破坏工业实体设备，企业无法借助以往的经验和手段对这类病毒进行查杀，设置的安全防护设施也无法及时发现这类病毒，只有对病毒攻击对象和被篡改的程序进行分析，阻断恶意行为指令才能避免病毒运行，从而保护工业网络。

二、网络技术背景下的工业网络安全防护

工业网络的有效应用具有十分重要的意义，能够为工业、企业的运作效率提升提供有效途径，还能为企业的经济发展提供有效依据。但是，基于网络实现运行，在一定程度上还存在较大风险。针对其风险的存在，如果不对其进行有效防护，将给企业的经济损失造成严重现象，在工业网络使用方式也会产生安全风险。其存在的问题主要表现在：

第一，硬件网络设备存在的风险。主要是其存在的交换机和端口。因为工业网络需要不断运行，受环境以及高温高湿度的影响，尽管设备自身性能好，但也会导致设备被损坏，该问题的产生一般在网络使用前期，所以，需要为其提供预案。比如：使用故障检测以及电源冗余手段等，能够维护工业网络在设备的有效运行。同时，针对数据传输期间存在的线路问题，其传输主要为光纤传输，对线路进行维护是十分必要的。比如：在煤矿井下，执行井下铺设的光缆通信线路，需要基于巷道进行铺设，以免产生通讯中断问题的产生。

第二，操作系统与杀毒软件的更新问题。工业网络在整体上都是内部网络，为了维护整体的安全性，需要将其与外部网络进行隔离，在该情况下，不仅会无法对网络进行计算，也无法对软件进行升级，从而带来明显的安全隐患。基于该问题的产生，需要专业的维护人员定期对系统进行杀毒

与升级。期间，升级工作的执行可以利用防火墙等安全设备，将其与外部网络进行连接。也可以利用专门的储存工具，在升级之前对系统进行备份，以免其产生不兼容问题。

第三，优盘、笔记本的导入会产生严重的病毒传播问题。内网设备在实际运行期间，也会应用一些优盘或者光盘等对资料进行传输和处理，从而导致工业网络在运行期间出现内部隐患。导致其问题的产生主要是病毒的感染，影响内网设备，从而给企业的整体运行造成较大危害。为了改变该问题，首先，可以在系统设置禁止系统的 USB 接口，并在内网电脑上设计比较复杂的密码。其次，对人员进行积极管理，可以在机房中设置访问登记制度，对其存在的故障进行处理，以免在储存介质中传入病毒。

第四，在工业控制系统，也会出现一些风险问题。当对工业控制系统的操作行为无法进行监控的时候，系统中将产生错误行为，影响工业控制系统的安全运行。所以，要为其建立有效的控制系统，对其进行监控与管理，保证能够对各个部分、各个环节进行监督。

第五，工业控制系统控制终端、服务器以及网络设备产生的故障如果没有发现，将产生明显的延迟问题。该问题的解决需要为其建立完善的监控系统，并将设备运行期间产生的各个参数集合在一个系统中，对服务器、网络设备进行合理监控，发现其存在的故障。在该情况下，不仅能促进控制系统的有效应用，也能对其存在的问题合理解决。

2.1 建构健全的安全信息管理平台

在网络技术的帮助下，若想保证工业网络安全性，可以从以下几个方面出发，首先规范数据类型，工业网络管理人员在工作当中要对收集的信息进行分类整理，之后进行整合并统一标准，将其存储于处理系统当中，如此无论数据是何种类型都可以借助自动化方式查询出来。其次，统一数据分类标准，工作人员在对收集的数据信息进行分类整理时首先要形成适合资源共享的分类体系，之后完善查询设施以减少查找过程中花费的时间，为数据处理提供便利帮助，同时确保分类合理。最后加强安全管理工具研发，工作人员要根据实际情况以及发展需求对安全管理工具进行研发，丰富其功能，以保护工业网络安全。

2.2 不断完善工业企业自身安全防御体系

随着网络技术应用范围愈发广泛，网络安全问题越来越多，工业网络若想保证自身安全必须不断完善防御体系，工业企业可以将相关软件安置在网络当中，例如网络安全滑动标尺模型等，该模型发挥的作用主要体现在以下几个方面：其一构建安全架构，在工业网络系统建立以及维护阶段，该模型能够为其提供保护；其二被动防御，如果工作人员没有对网络进行操作，该模型可以为网络提供维修防御；其三积极防御，该模型运用过程中可以监控网络运行过程中受到的安全威胁，并对其进行分析。其四情报，该模型可以将工作人员收集的数据转化为信息，同时对其进行处理以此弥补数据资源方面存在的缺陷。其五进攻，在法律的帮助下对某些非法攻击行为进行反击。

2.3 基于威胁情报的工业网络安全态势感知

工业网络运行过程中很难生产威胁情况，通常需要经过以下步骤：了解数据基本信息这是威胁情报生成基础；整理数据将不准确数据剔除；梳理不同数据之间的关系；借助机器验证数据准确性；情报要包含报警内容；根据情报信息划分报警等级；以分发为主体，采取特殊格式输出情报，例如 xml、STIX 等，在该阶段有一点需要注意，如果情报类型并不属于 MRTI 范畴，则可以使用 Word、PDF 完成输出；结合实际需求灵活运用情报，以此推送产品，收发邮件。

2.4 实现工业内网安全管理可视化

在网络技术的帮助下，安全管理可视化对工业网络安全具有非常重要的作用，对不同数据之间的联系进行探究不仅能够提升分析人员业务能力，同时工作压力也会减轻。具体可从以下两个层面入手，其一数据结构化，工作人员在操作工业网络过程中可以利用安全管理可视化技术整合碎片数据形成结构，例如异常警告等，以此来实现可视化管理提高实用性；其二实现有机结合，该技术运用过程中，威胁事件能够与业务结合在一起，而这种模式无疑使工业网络更加安全直观，能够及时发现隐藏在其中的安全隐患，有助于保护工业网络安全。

结语：综上所述，文章主要以网络技术为背景对工业网络安全防护进行分析探究，可以看出在时代变化社会进步过程中，工业网络已经成为核心部分。但是在运用过程中却经常受到各种不可控因素的干扰，导致安全性降低，甚至出现信息外泄等情况。影响工业网络安全性的因素有黑客攻击，操作不当，病毒等，为此企业可从可视化管理、构建安全信息管理平台、完善防御体系等多个角度入手为工业网络提供保护，在网络技术的影响下提高工业网络安全管理水平。工控系统产生的安全问题给当前的生产安全造成加较大威胁，也导致企业面临严峻的经济损失。所以，各个政府需要加大力度实现工业控制系统的安全管理工作，将企业的安全和效益作为重点，解决其存在的各个问题，促进网络的有效应用，保证能够避免其风险的产生。

参考文献

[1] 雷邦兰，龙张华 . 基于大数据背景的计算机信息安全及防护研讨 [J]. 网络安全技术与应用，2016.

[2] 孙红梅，贾瑞生 . 大数据背景下企业网络信息安全技术体系研究 [J]. 通信技术，2017.

[3] 杨艳，张莹 . 大数据背景下的网络信息安全研究 [J]. 自动 | 化与仪器仪表，2016.

[4] 尚进 , 谢军，蒋东毅 , 陈怀临 . 现代网络安全架构异常行为分析模型研究 [J]. 信息网络安全 ,2015.9:15-19

[5] 董梦林 . 大数据背景下网络信息安全控制机制与评价研究 [D]. 吉林大学硕士学位论文 ,2016.5.