

数字化转型背景下制造业网络安全的挑战与应对对策研究

李 明

(广州城建职业学院, 广东 广州 510925)

摘要：随着现代产业的不断变革和信息技术的不断发展，制造业与信息技术的融合如今已经越来越深入。国务院印发的《关于深化“互联网+先进制造业”发展工业互联网的指导意见》指出，“工业互联网”是数字化转型背景下制造业与新一代信息技术深度融合的重要产物，同时也是推进我国加强网络强国建设的关键支撑和基石。目前，各种不同类型的工业互联网平台不断涌现，越来越多的设备也接入了网络，这虽然在一定程度上促进了制造业的信息化转型，但同时也使得制造业控制系统的网络安全问题日益突出。基于此，本文主要针对数字化转型背景下制造业网络安全的挑战及其应对展开了相关分析与研究，仅供参考。

关键词：数字化转型；制造业；网络安全；挑战；应对对策；创新

在数字化转型背景下，针对制造业领域控制系统的网络攻击手段层出不穷，信息安全、网络安全等问题的频发无疑会给其生产和运行带来巨大的风险。所以，面对如此巨大的网络安全风险，制造业领域有必要充分认识到当下存在的网络安全问题，并积极采取相应的应对措施，构建相应的安全信息架构，以保证自身的长远、稳定发展。

一、数字化转型背景下制造业网络安全的挑战

(一) 生产设备安全问题开始凸现

在传统的制造业生产中，所用的大多都是机械设备，其管理和维护的重点更偏向于物理和功能安全。然而，在数字化转型背景下，制造业生产模式在信息技术的辅助下发生了明显转变，这就会让生产设备逐渐向智能化、信息化、网络化、数字化发展，最终会大大减少制造业生产过程中的人机交互行为。虽然这可以很好地保证生产人员的安全，但这也暴露出这样一个问题，即：大量的生产设备直接暴露在网络攻击和威胁之下，一旦这些设备受到了木马病毒的攻击，那么就可能会迅速、大范围瘫痪。

(二) 端到端生产模式的网络安全问题

为进一步提高生产效率，越来越多制造业企业开始在互联网的支持下承担起“端到端”的服务，包括生产、产品交付以及运维管理等。在数字化转型背景下，服装行业、家电行业等开始为人们提供个人定制服务，实现了“端到端”生产服务模式的转型。但这种无任何的生产模式，无疑大大增加了企业生产的网络安全问题。例如，工业网络灵活组网的需求越来越丰富、多样，这就容易导致其网络拓扑结构越来越复杂，进而就会大大降低传统制造业静态防护和安全域防护的效果。另外，在生产过程中，网络信息也可能会被泄露，网络钓鱼攻击行为日益突出等，这也是数字化背景下制造业网络安全管理过程中需要面对的一个重要问题。据 2023 年数据显示，网络钓鱼攻击事件总数约为 16 亿起，同比增长 166%，其中主要集中在制造业、服务业、医疗行业和教育行业等行业。其中，制造业尤为突出，占比 27.5%（见图 1）。

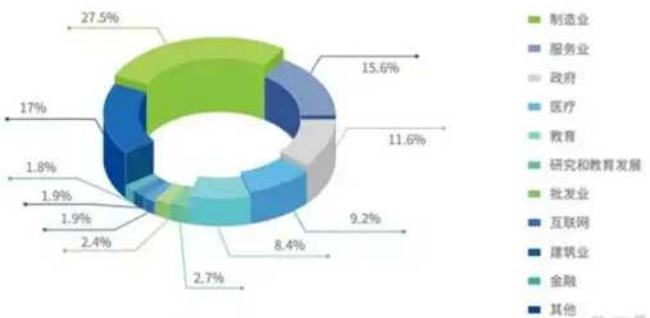


图 1 各行业网络钓鱼攻击占比

(三) 工厂控制安全问题

目前，我国制造业企业生产管理中的安全管理主要集中在控制过程的功能安全上，二对于信息安全的防护能力还需进一步加强。就现阶段来看，企业所使用的控制协议、控制软件等，基本上都是建立在信息技术、运营技术相对独立以及运营技术相对可靠的基础上。但是，在实际生产过程中，制造业企业对于控制系统的实时性、可靠性等往往有着更高的安全管理要求。而在数字化转型背景下，信息技术与运营技术的融合愈发深入，显然，这势必会对传统制造业企业生产加工过程中的安全可信控制环境造成一定的冲击和影响，极有可能引发从信息技术层向运营技术层的网络攻击问题，进而使得网络安全问题由企业外部向企业内部蔓延。并且，更令人担忧的是，工厂控制安全问题从某种程度上也会对现实的物理空间带来一定安全隐患。但事实上，制造业领域目前还尚未探索出能够有效应对高级持续性威胁攻击的检测与防护手段，这也是数字化转型背景下制造业改革发展过程中需要解决的一大难题。

(四) 应用和数据安全问题

个性化定制、网络化协同、服务化延伸等一些列新模式、新业态的出现和应用，这无疑对传统公共互联网的安全管理能力提出了更高的新要求。而且，在数字化转型背景下，工业互联网的数据体量不断增加，种类越来越多，结构愈发复杂，数据流动也开始从单向转变为双向，这不但会在一定程度上影响网络信息传递的实时性，而且还会大大增加重要制造业数据的应用与保护难度。

二、数字化转型背景下制造业网络安全的应对对策

(一) 加强互联网安全实验室建设，实现关键软硬件自主研

发

在数字化转型背景下,制造业需要加大互联网安全实验室的建设力度,积极为企业的生产和运行搭建安全的作业环境,同时还要与科研院、相关制造厂商等取得合作,集多方主体的力量自主研发相关关键软硬件产品,并做好安全测评,从而更好应对数字化转型背景下的诸多网络安全问题。

(二) 加强互联网安全技术手段建设,提高关键工业设施安全防护能力

制造业需要充分发挥互联网安全技术手段的优势,积极打造国家工业互联网安全漏洞共享平台,借此来促进相关网络安全信息的共建共享,比如安全漏洞、安全风险、安全预警等信息,并建立健全的网络安全风险通报机制,从而更好地保障企业数字化转型升级。与此同时,制造业还要结合行业特点,建设工业信息安全模拟仿真平台和安全监测预警平台,用于支撑信息安全检查、网络安全事件通报与响应等管理工作。

(三) 转变互联网安全防护的思维模式,促进安全防护的智能化发展

企业要树立良好的互联网安全管理与防护思维,促进安全事件响应模式智能化转变,同时还要加强对人工智能技术、大数据分析技术等学习与运用,积极建设安全数据资源库,从而进一步提高对高级威胁的预测、防护、响应与恢复能力。

另外,企业还要创新网络安全信息架构,促进其向智能化、自动化升级发展,从而构建更加完善的安全防御系统。制造业企业可以根据行业特点建立如下信息安全架构体系,从而实现对自身的整体性安全防护、综合性态势感知、自适应安全防御和动态安全管理。具体来看,安全架构的构建应立足国家政策与行业生产标准和控制要求,尽可能覆盖制造业控制、终端、网络、业务及应用等各个方面,主要有技术保障体系、政策体系、安全标准体系、安全管理与运维体系等。

(四) 增强对互联网大数据的分类分级保护流动追溯

在数字化转型背景下,工业大数据得到了迅速发展,因此,制造业行业企业对于相关数据的分类、分级保护要求有所提高,尤其更注重用户隐私、大数据分析价值等的保护。在此形势下,制造业行业企业还需将对网络数据的分类、分级保护及其流动追溯等作为网络安全防护的重点。

三、数字化转型背景下制造业网络安全的基础保障

(一) 加强顶层规划

近些年来,虽然我国为促进工业信息安全工作的有效落实出台了政策和法规,但大多数的安全政策是聚焦于工业互联网领域,相较而言,对于工业信息安全技术产品体系、人才培养体系等的统筹规划力度还不够。所以,在数字化转型背景下,为进一步加强制造业信息安全顶层设计,国家层面还需加大财政与政策的支持力度,除了要持续完善新兴制造业领域工业信息的安全法律、管理政策、标准体系以外,还要规范和指导相关企业对于新技术的应用,借此来不断提高企业网络安全管理意识与安全防护水平,从而充分发挥出国家对于制造业数字化转型的引领与规范作用。

(二) 重视公共服务

安全公共服务是保障制造业工业信息网络安全的一项重要举措,可以有效降低企业遭受网络攻击的风险,进而达到提高企业安全能力的目的。在数字化转型背景下,该服务可以以在线服务

等方式来实现,能够为制造业行业企业提供各种网络威胁(如安全漏洞、病毒、木马蠕虫、恶意攻击等)安全实时监测与应急处理管理服务,有利于促进网络安全实现线上线下协同管理,从而大大提高管理的效率和效果。不过,需要注意的是,当前我国制造业工业信息网络安全公共服务的资源库建设标准尚未统一,对于数据信息的可靠性和隐私性保护力度还不够,网络安全应急响应系统还未规范化。针对这些问题,制造业可以借助互联网,加强对各类网络安全资源的有机整合,不断提高信息资源共建共享程度,从而帮助更多企业建立更为完善、有效的网络安全防护与管理体系。

(三) 推动试点示范

随着社会时代的不断发展,我国已经深刻意识到推动试点示范的重要性。为此,在制造业数字化转型的发展进程中,我国工信部不仅开展了一些列的工业互联网试点示范项目推荐工作,而且还发布了信息技术与制造业融合发展试点示范相关工作通知,旨在通过试点先行和示范引领,从中总结出更多可复制的优质经验和做法,以便更好地支撑制造业数字化转型与升级。然而,在试点示范工作的实际推进过程中还存在一些问题,如有的企业缺乏行业技术规范标准;有的企业网络安全体系的建设还不完善,基础设施和设备的升级优化进展缓慢等。面对这些问题,国家层面应当进一步完善制造业行业标准体系。而相关企业则要立足于提升工业安全控制系统的本质,加强对该系统的升级与改造,并结合自身实际和业务特点来针对性提升自身的网络安全风险检测能力、防范能力和消减能力,同时还要做好相关经验总结,从而达到以试点示范有效促进制造业网络安全管理能力提升的目的。

(四) 加强人才培养

在数字化转型背景下,制造业网络安全风险的检测、防护与管理离不开人才的支持和保障。所以,社会各界还需充分发挥各自的资源优势,加强人才培养。例如,国家和地方政府应当建立健全的系统化人才培养机制,做好人才发展规划,用于指导地方院校、科研机构以及相关企业开展人才培养工作。各地方院校以及科研机构则要加强学术交流和学科建设,积极创新人才培养模式,从而为国家和社会输送更多高技能人才。工业企业和安全企业则要充分发挥各自的专业优势,利用技能竞赛平台与学校合力培养复合型工业信息安全人才。

四、结语

总而言之,在数字化转型背景下,安全是制造业实现数字化升级与发展的重要前提和基本保障。只有构建更为全面的安全防护体系,才能有效识别并抵御各种网络安全威胁,才能更好地化解网络安全风险,最终促进制造业健康、有序、长远、稳定发展,从而为我国制造业的数字化转型和升级提供更多助力。

参考文献:

- [1] 杨光. 制造业企业从七个方面发力做好网络安全防御 [N]. 中国信息化周报, 2024-04-29(022).
- [2] 陈仕意. 网络安全——数字化转型发展的压舱石 [J]. 计算机仿真, 2024, 41(05): 400-404.
- [3] 李琛, 董诗婕. 5G 赋能密码护航推动传统制造业安全高质量发展 [J]. 中国水泥, 2023, (05): 26-29.

此论文成果用于支撑广州城建职业学院校级课题《基于 Fuzzy-ISM 的老年“数字鸿沟”视角下城市数字化转型研究》研究