浅析数字化转型浪潮下的网络安全体系构建

姚拯

（上海民航新时代机场设计研究院有限公司，上海　200335）

摘　要：数字化转型作为重要发展战略与经济驱动力，在信息化的基础上进一步把信息技术与业务运营、管理流程融合在一起形成了新的业务运营模式，显著提升了业务运营效率和效益。在数字化转型带来巨大收益的同时，业务数据与数字化的深度融合对网络安全也提出了更高的要求，一旦网络安全遭受攻击，将会对业务运营带来破坏性的打击，应对网络安全风险也就等于面对业务运营风险，如何构建网络安全基础设施和实战化运行体系，实现全方位的网络安全防御能力体系，从而保障数字化业务安全成为了全新的课题。然而网络安全体系从建立到实现不是一蹴而就的，需要循序渐进的逐渐积累，从根本观念的转变、整体层面的规划，对现有问题的分析，补齐短板，夯实安全基础，再到深化安全能力，构建主动防御模式，进而实现智能协同，深化动态防御理念，最终达到深化数据安全全生命周期安全防护的目的。

关键词：数字化转型；网络安全；物理隔离

0　引言

网络安全和信息化是一体之两翼、驱动之双轮。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。明确了“统一谋划、统一部署、统一推进、统一实施”缺一不可的体系化建设要求。

1　背景

随着信息化进程的深入，我国已逐步由信息化进入了数字化转型期，层出不穷的新技术应用给业务运营带来了更多的安全风险，与此同时信息技术与业务运营的深度融合也使网络安全风险更具有实质性的意义。

在对数据依赖性逐渐提升的环境下，网络攻击是全球各国都面临的问题，尤其是电力、通信、能源化工等关键基础设施。全球范围内面对网络攻击事件中均暴露出网络安全体系化欠缺的现状，为各行业敲响警钟-网络安全风险等同于业务运营风险。信息系统一旦被黑客侵入或被破坏，将会直接危害到业务运营，网络安全是关系着国计民生的大事。

自我国推行网络安全等级保护制度以来，国家有关部门相继颁布了《网络安全法》、各类安全保护条例以及相关指导意见，明确关键信息基础设施行业和领域范围是我国网络安全保护的重中之重。

2　需求分析

从信息化到数字化的发展历程中所采用的IT体系规划：企业架构（EA）方法论以及服务管理、运维管理（ITIL）理念对信息化发展起到了很大的作用，使得业务运营体系向大规模、体系化、高效整合方向发展，如图1所示。

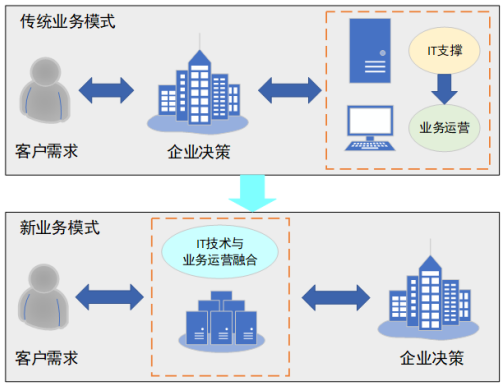

图1　业务运营模式的转变

而在网络安全领域缺乏与之同等层次的思维引导规划和方法理论，在各系统建设的初期未考虑同等级别的网络安全，将网络安全作为后台的保障措施，致使现有网络安全碎片化严重、协同能力差，传统的模式已无法支撑数字化转型背景下的网络安全要求，必须从根本上转变理念，以全局性网络安全观构建网络安全体系。

3　网络安全防护存在的问题

数字化转型的时代背景下使得大数据技术在各行各业的应用已经越来越广泛，业务运营相关的信息和数据经网络传播的途径和方式也越来越多样化，面对日益严峻的网络威胁，以往所用的网络管理方法和防护技术无法满足大数据时代的网络完全要求和网络特点[1]。然而网络安全所面临的威胁不仅仅来自于外界，还来自于对网络安全防护理念的不重视，过分依赖物理隔离方式以及对内部潜在威胁的忽视。

3.1　缺乏体系规划

自2006年我国推行网络安全等级保护制度以后的10年里，虽然逐步建成了基础性的安全防护体系，开启了《等保1.0》时代，保障了以往业务的运行，但对于一些领域的管理仍处于起始阶段，顶层设计相对薄弱，影响了我国网络安全体系的构建[2]。缺乏统一的网络安全体系规划，致使各部门在网络安全建设和管理上各自为政。

3.2　依赖物理隔离

在民航领域，物理隔离一度被广泛应用，认为对内外网进行物理隔离就可以从根本上杜绝网络安全的隐患，却忽视了随着技术的发展，各类高新入侵技术一旦攻破了物理隔离网络侵入信息系统内部，将不再有相适应的防御手段。此外，重设备而轻运营的观念使得初期的高投入与后期防护效果无法匹配，甚至于产生轻视和松懈的心理，使得防御能力形同虚设。

4　网络安全体系构建

自2017年《网络安全法》生效伊始，有关部门相继出台了各类相关的条例及指导意见，加大对网络安全体系建设的力度，使得我国网络安全保护已逐步进入了《等保2.0》时代，对于网络安全体系的构建可从以下几个方面进行。

4.1　观念模式转变

落实“四统一”，加强网络安全防护工作，从“局部整改”、单一系统防护模式转变为体系化规划建设模式，以系统工程方法论来指导网络安全体系的规划、设计和建设工作，保

护数据安全的同时，对相关人员、系统应用、数据整合以及运行支撑体系之间的交互关系进行整体防护。

从完善基础设施建设开始，由原来的被动防御向主动防御转变，进而在早期做出对威胁情报的响应，以“关口前移，防患于未然”的网络安全能力为导向，进行规划设计，构建技术、运行、管理体系三位一体的安全保障体系来支撑网络安全能力从而达到保障生产业务的目的，如图2所示。

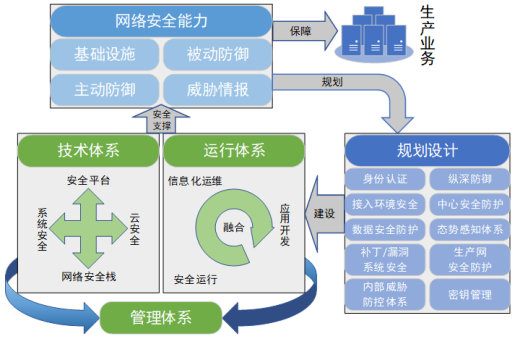

图2　网络安全体系总体框架

4.2　体系化规划

网络安全体系的构建与业务运营的战略规划以及安全设备建设方案息息相关，体系化规划可以起到承上启下的关键性作用，它既要符合网络安全相关法律法规的要求，契合业务运营的战略思想，又应促进安全标准在数字化建设项目中得以融合，有效的指导具体的方案得以落地实现，如图3所示。避免以偏概全的传统模式，以全覆盖、层次化思路进行统筹规划设计，建设动态综合的网络安全体系，使安全防护能力从技术、管理、运行等各层面覆盖系统、网络、安全设备、人员管理、运营保障等要素，避免因局部盲区而导致的防御体系失效，形成多维度有效集成，提升保障能力。

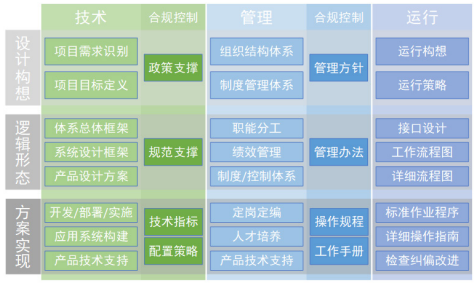

图3　安全保障体系规划结构图

4.3　规划先行分步建设

科技发展过程中所遗留的问题并不能在一次或几次大规模建设中就得到解决。从资源利用角度来说，一味的推翻过去的成果也是不可取的，充分了解业务需求，结合现有设备与新安全防控技术的优势，从顶层出发先行做好整体规划部署，合理调配资源，以防控要点防御薄弱点为重点开展分步建设，依据业务运行的具体需求，在规划阶段确定需求和建设阶段的划分，使网络安全体系建设工作能够得到充分的保障和有力推动。

同时建设也应本着“宁可备而不用，不可用时无备”的原则，以可扩展的模式进行建设，在业务运行中预留必要的冗余安全能力，确保在面对网络安全突发性风险时，能够尽可能降低网络安全隐患给业务运营带来的影响。

4.4　零信任架构及应用

数字化转型以及疫情的影响推动了远程办公，为各行各业带来了新的生产力和工作模式，但也同时给网络基础设施带来了挑战，数字化浪潮正逐渐瓦解网络安全边界，传统基于边界的安全解决方案已难以适应。为了应对日益严峻的网络威胁形势，零信任架构应运而生，用“从不信任，总是验证”的理念来解决现今网络边界消弭现象，是构建网络安全体系的关键技术，如图4所示。

零信任的本质是在访问主体和客体之间构建以身份为基石的动态可信访问控制体系，其理念的建立基于以下三个方面：网络始终处于危险的环境中；网络始终面临内外部威胁；网络位置不足以决定网络的可信度[3]。

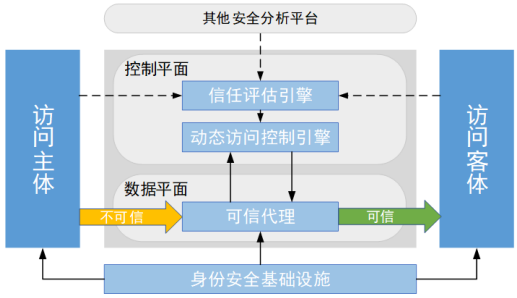

图4　零信任防护参考架构

零信任架构的关键能力是基于以对访问身份为基石，通过对业务访问请求进行全流量加密、认证和强制授权，进行持续的信任评估，最终通过动态访问控制形成安全闭环能力，在主客体之间建立一种动态的信任关系。

零信任架构灵活的实现方式和部署模式可以应对不同的应用环境和业务场景。例如随着数字化转型，远程办公、远程业务开展、远程运维、远程开发的逐渐常态化，零信任安全架构针对此类远程访问应用场景，采用去边界化思维方式，不再简单的区分内外网，转而注重于对核心业务和数据资产的管理，在人员、设备以及业务之间构建动态访问控制体系。

以远程办公为例，远程访问存在的主要网络安全风险包括：访问的设备存在安全隐患、云桌面自身所存在安全漏洞以及静态授权机制下无法实时响应风险，当远程客户端发生异常操作、非授权访问等行为时，无法及时阻断访问以降低风险。为了解决上述问题，给出远程访问零信任建议方案如图5所示。

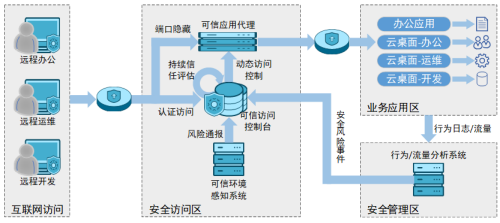

图5　远程访问零信任防护建议方案

通过部署零信任方案可以完成风险通报、对访问的持续信任评估、行为日志以及全流量的分析，实现以最小信任度进行远程客户端的接入，从而达到远程动态访问的目的。

4.5　安全运营体系建设

想要全面提升网络安全防护能力，除了网络安全体系的构

建、防控技术手段的应用，安全运营体系的建设也是至关重要的，没有安全运营体系的落实，再好的规划，再先进的技术也无法发挥出其应有的效用。如何落实安全运营体系，首先要明确运营不等于运维，如果说运维可以理解为设备技术可用，那么运营就是从可用的设备技术中充分发现价值。

运营工作不是一蹴而就的，应当运用质量管理体系PDCA循环理论把安全体系的整体规划设计作为安全研究（Plan）；把安全基础设施建设作为安全建设（Do）；把防控技术手段所提供的安全审计、安全评测、安全监测等服务作为安全服务（Check）；把逐步完善安全防护、安全管理、安全评价体系作为安全优化（Action）周而复始的对安全运营进行持续投入与技术迭代，才能形成网络安全体系的闭环运营。

充分结合人、数据、工具、流程，才有可能实现安全运营的目标。安全运营最终还是要能够清晰的了解业务运营的安全情况、发现安全威胁、敌我态势、规范安全事件处置情况，提升安全团队整体能力，逐步形成适合业务运营的安全运营体系，并通过成熟的运营体系驱动安全管理工作质量、效率的提高。

5 结论

数字化和信息化进程的不断加快，数据的应用以及业务模式逐步走向多元化，对数据的保护使得网络安全显得更加重要。为了建设与数字化业务标准相匹配的网络安全体系，彻底改变传统局部改造、以产品堆叠为主的规划模式，应当从全局出发，利用系统工程方法论指导网络安全建设，将安全与数字化进行深度融合，为数字化转型提供强有力的安全防护盾，从而实现全方面的网络安全防御能力体系，保障数字化业务安全、平稳、可靠运营。

参考文献

[1] 李明杰 , 张英华 . 大数据时代计算机网络安全体系构建 [J]. 中国管理信息化 ,2020,23(02):148–149.
[2] 王迈为 . 网络安全防护体系构建问题研究 [J]. 网络空间安全 ,2017,8(Z2):32–35.
[3] 左英男 , 张泽洲 . 基于零信任架构的远程移动办公安全体系及应用研究 [J]. 保密科学技术 ,2020(03):36–40.

（上接第215页）

背后其实是商家，商家和企业要担负社会责任，加强商品质量的把控，不以次充好，不夸大其词，做好产品售后工作，提供干净健康的消费环境。

3.2 加强网络环境的净化

如今很多网红短视频在宣扬一种奢侈消费的观念，对大学生消费观念的形成带来了很大的负面效应。像快手，抖音，西瓜视频等大型短视频平台要加强监管，减少三观不正的视频流出。发挥媒体的舆论导向作用，宣扬正确的消费观念。网络直播带货要逐渐完善起来，从选品到售后都要严格把控。媒体的报道以宣扬合理消费为主，担起社会责任，对网络安全进行普及和宣传。

3.3 大学生要树立正确的消费观念和消费行为

不盲目跟风，不攀比，不超额消费。提高警惕，不贪图小便宜，不受别人的蛊惑，提高自我防范意识和防诈骗意识；努力学习科学文化知识，懂得法律知识，当自己的权益受到侵害时要学会用法律武器保护自己。

4 结论

新媒体的出现既给我们的生活带来了便利，同时也给我们带来了潜在的威胁，对大学生的消费行为和消费观念带来的影响既有正面也有负面。净化新媒体环境、加强网络环境净化是一件很有必要的事，当然大学生自身也要树立好正确的消费观，量入为出适度消费，避免盲从，理性消费。

参考文献

[1] 余启东 , 许冰悦 . 新媒体经济下大学生时尚消费观念及行为探析 [J]. 电视指南 ,2018(11):225–226.
[2] 马晓利 . 分析“90 后”大学生消费心理与行为现状 [J]. 智库时代 ,2019(23):29–30.
[3] 林力宇 .90 后消费趋势分析 [J]. 现代营销 (经营版),2019(6):120.
[4] 黄潇潇 . “90 后”大学生消费行为的思考 [J]. 知识经济 ,2018(1):128.