公司代码:688168　　公司简称:安博通

北京安博通科技股份有限公司 2019年年度报告摘要

一重要提示

1本年度报告摘要来自年度报告全文,为全面了解本公司的经营成果、财务状况及未来发展规划,投资者应当到上海证券交易所网站等中国证监会指定媒体上仔细阅读年度报告全文。

2重大风险提示

公司已在本报告中详细描述可能存在的风险,敬请查阅第四节“经营情况讨论与分析”部分“可能面对的风险”的内容。

3本公司董事会、监事会及董事、监事、高级管理人员保证年度报告内容的真实、准确、完整,不存在虚假记载、误导性陈述或重大遗漏,并承担个别和连带的法律责任。

4公司全体董事出席董事会会议。

5大信会计师事务所(特殊普通合伙)为本公司出具了标准无保留意见的审计报告。

6经董事会审议的报告期利润分配预案或公积金转增股本预案

公司2019年利润分配方案为:以公司总股本51,180,000股为基数,向全体股东每10股派发现金红利4.5元(含税),预计派发现金红利总额为23,031,000元(含税),本次不进行资本公积金转增股本,不送红股。本次利润分配方案需经公司2019年年度股东大会审议通过后实施。

7是否存在公司治理特殊安排等重要事项

□适用 √/不适用

二公司基本情况

1公司简介

公司股票简况

√适用 □不适用

公司股票简况				
股票种类	股票上市交易所及板块	股票简称	股票代码	变更前股票简称
A股	上海证券交易所科创板	安博通	688168	不适用

公司存托凭证简况

□适用 √/不适用

联系人和联系方式

联系人和联系方式	董事会秘书(信息披露境内代表)	证券事务代表
姓名	夏振富	杨帆
办公地址	北京市海淀区西北旺东路十号院东区15号楼A座301	北京市海淀区西北旺东路十号院东区15号楼A座301
电话	010-57649060	010-57649060
电子信箱	xiazf@abtnetworks.com	xiazf@abtnetworks.com

2报告期公司主要业务简介

(一)主要业务、主要产品或服务情况

1、主要业务

公司主营业务为网络安全核心软件产品的研究、开发、销售以及相关技术服务,为网络安全行业网络安全系统平台与安全服务提供商。在网络安全行业中,发行人依托于自主开发的应用层可视化网络安全原创技术,为业界众多网络安全产品提供操作系统、业务组件、分析引擎、关键算法等软件产品及相关的技术服务。

2、主要产品

(1)嵌入式安全网关

嵌入式安全网关主要用于数据通信网络环境,是一种软硬件结合的实体安全设备,通常用于网络互联网出口或网络关键区域边界,是网络中用于隔离、控制、防御的基础安全产品,嵌入式安全网关包括下一代防火墙及网络行为管理与审计等组件与产品。

下一代防火墙产品采用先进的高性能并行架构,保障业务处理高效可靠,场景支撑灵活全面。产品具备应对高级持续性威胁的入侵防御能力和实时病毒拦截技术,将访问控制模块与漏洞扫描、Web防护、入侵防御、沙箱仿真、数据防泄漏、威胁情报等系统形成智能的策略联动,通过并行处理的深度安全检测引擎和应用识别技术,实现对用户、应用和内容的攻击行为深入分析,为用户提供安全管理的一体化防护体系。

网络行为管理与审计产品提供全网终端统一管控功能,具备传统认证和主流社交软件等身份认证方式,保障用户接入安全可控。该产品内置千万条URL库和五千条主流应用行为特征库,配合网络行为管理策略模板,可实现网络行为精细化识别和控制。该产品通过智能流量管理特性,动态分配空闲时带宽资源,帮助用户提升用户上网体验。该产品结合清晰易用的管理日志功能,为企业提供全面、完善的网络行为管理解决方案。

为满足客户的不同需求,嵌入式安全网关产品对外提供嵌入式软件系统与嵌入式软硬一体化产品两种产品形态,其中软件系统提供给部分客户与其已有硬件相适配,软硬一体化产品为软件加硬件搭配的一体化安全网关产品。两种产品形态相辅相成,为客户提供全面、灵活的产品形式。

(2)虚拟化安全网关

虚拟化安全网关产品通过虚拟化技术将安全防护特性与虚拟计算、虚拟存储、虚拟网络适配并融合到通用服务器中,形成标准化的防护单元,多个防护单元通过资源池方式汇聚成数据中心整体安全架构,并通过统一的管理平台实现可视化集中运维管理。

虚拟化安全网关以通用服务器为硬件载体,主要应用于大型数据中心和云计算中心,以安全资源池的形式满足公有云、私有云、混合云等多种云场景下的安全需求,并通过统一的管理界面实现全网安全资源池的分配和调度,主要用户包括政务云数据中心、运营商数据中心、金融数据中心和公有云服务提供商等。

(3)安全管理产品

安全管理产品主要包括扬流量可视化、策略可视化、云安全管理产品等。针对新型的网络攻击手段与高级持续性威胁,通过采集网络中各类网关设备与监测设备产生的数据与流量,运用安全大数据分析、深度机器学习与流量可视化技术,发现并阻断网络中传统技术无法检测出的违规行为与未知威胁,这些产品已经成为构建网络安全态势感知系统的重要组成部分,依据国家网信部门网络安全监测预警和信息通报制度的技术要求设计,部署在网络管理集中监控位置,通过大屏显示系统呈现和运维管理。该产品利用数据融合、数据挖掘、智能分析和可视化技术,直观显示网络环境的实时安全状况,对潜在的、恶意的网络攻击行为进行识别和预警,提升安全设备的整体效能,具备网络安全管理和预判能力,为网络安全提供运维保障。

3、服务情况

目前,公司网络安全服务主要为安全产品技术开发与安全运维服务,根据客户的个性化需求,在公司主营产品基础上定制开发扩展功能或个性化功能,或按照定制化需求开发产品特性或提供解决方案,同时提供产品运维保障服务。

(二)主要经营模式

公司自成立以来,坚持做网络安全能力的提供者和技术支持者,定位于网络安全行业上游软件平台与技术提供商,为行业内产品与解决方案厂商提供产品或服务。

1、研发模式

公司坚持自主原创、自主创新的研发策略,核心产品和关键技术主要来源于内部创新与自主研发。公司各产品线研发主要以ABT SPOS平台为基础,为客户提供稳定可靠的产品,满足客户需求。公司产品的研发过程分为需求提出、需求筛选、开发测试、发布宣传等四个阶段。客户服务人员在和客户的维护联系过程中,将不同客户的需求提交给产品部门,产品部门要对这些需求进行评估,包括可见的市场容量、研发需要的耗时等,以确认是否列入研发计划。所有需求都会被记录,一些紧迫的、重要的、共性的需求会规划到公司产品的研发计划中,在产品各版本中体现。公司通过前期的需求分析和筛选,确保开发的产品符合市场需求并具有广阔的应用前景;通过产品的开发与测试,确保产品质量以及功能上满足市场需求。

为有效管理研发项目、对研发费用进行准确核算,公司制定了《研发项目管理制度》、《设计开发程序控制制度》和《研发费用管理制度》。公司产品研发须经过市场调研、立项、设计、开发、测试、验收与发布等几个阶段,具体流程为:由产品部根据市场调研结果提出研发需求,由研发部拟定项目计划书,经产品管理委员会审批,报公司总经理批准后立项,立项后由研发部会同财务部编制项目预算,由研发部具体组织实施并对研发全流程进行跟踪管理。产品管理委员会组织验收,再由产品部发布产品,以确保对研发费用的准确核算。公司按研发项目设立明细账归集相关项目研发支出,并按费用性质进行明细核算。

2、采购模式

公司采购的生产用物料主要包括嵌入式网络通信平台及服务器,对嵌入式网络通信平台采用定制化采购;服务器为通用型标准化产品,公司根据需求对服务器进行直接采购。

在嵌入式网络通信平台采购中,公司产品部根据需求制定硬件平台的设计要求,包括硬件外观、各项参数指标等,由合格供应商提供满足设计要求的硬件产品,并经公司对其与嵌入式安全网关软件运行测试合格后进行批量采购。

公司建立了《采购与付款制度》以规范采购行为,生产用物料的采购主要由供应链管理部门执行,由产品部及商务部等辅助完成。

(1)供应商的选择

公司根据产品需求对能够提供合格产品的供应商发出合作邀请,产品部根据多家供应商提供的产品进行测试评估,根据测试结果初步筛选2-3家可选供应商。公司综合考虑可选供应商的产品质量、产品报价、供货能力、售后服务、供应商实力等因素择优确定合作供应商。

(2)采购流程

经测试,公司所需硬件产品达到批量生产标准后,供应链管理部门根据商务部反馈的销售订单量和对部分客户提供的销售预测制定采购计划,在系统中提交《采购申请单》,经由财务部及总经理审批通过后,供应链管理部向供应商下达正式采购订单。对于嵌入式网络通信平台,供应商按照公司采购订单安排生产,经验收合格入库;对于服务器产品,供应商按公司要求直接发货给客户。

3、生产模式

公司产品有纯软件产品和软硬一体产品两种形态。

对于纯软件产品,公司产品研发部门进行软件系统研发,测试部门负责对软件版本进行调试检测无误后将软件系统刻录到光盘等存储介质寄送客户,或保存在公司服务器中由客户自行下载并记录使用数量,由公司提供序列号给客户激活使用,期间严格把控产品及售后服务质量。

对于软硬件一体化产品,其中硬件设备全部为外购,公司向供应商采购硬件设备后,将软件产品灌装到硬件设备中,通过调试和检测后,交付给客户使用。由于公司的硬件产品标准化程度较高,为提高产品的交付时效、减少中间运输环节,公司对大部分客户采取供应商直运模式,由供应商将公司软件灌装到硬件设备,最终由公司对产品检测合格后对外销售。

4、销售模式

公司坚持定位于做安全能力的提供者、上游软件平台与技术提供商,通过直销模式向行业内各大产品与解决方案厂商销售网络安全产品或提供网络安全服务,专注于做网络安全行业上游网络安全软件系统的提供商。

公司提供的产品作为一项专业性较强的标准化产品,客户选择公司产品之前,一般会对公司产品的各项指标进行测试,包括功能测试、适配性测试、稳定性测试、易用性测试、隐私和安全性测试及性能测试等。客户按照其各自需求,测试的侧重点不同。在客户获得满意的测试结果后,双方就产品价格进行谈判协商确定,并约定产品交付时间、交付地点及付款信用期等主要事项。对前述事项达成一致后,双方签署合作合同,公司承担向客户转让商品的主要责任。

公司建立了《销售与收款制度》以规范销售行为,销售流程按照销售内控制度执行。公司具体销售流程介绍如下:

客户根据其需求向公司商务部提出产品采购需求,商务部将审批后的销售合同/订单信息录入ERP系统中,经商务部经理审核通过。

针对软硬一体化产品,商务部根据审核通过的销售合同/订单信息确定交货期后,向仓管人员下达发货指令,仓管人员根据发货指令发货,客户收货确认方式主要包括两种:一是通过与对方对账确认;二是通过对方签署的收货确认单据确认。商务部将收货确认相关的销售合同/订单、物流单、收货确认单或对账单等原始单据转交给财务部,财务部据此确认收入并入账;同时经总经理审批通过后,由财务部开具发票。商务部根据双方约定的信用期,跟踪应收账款回款情况。

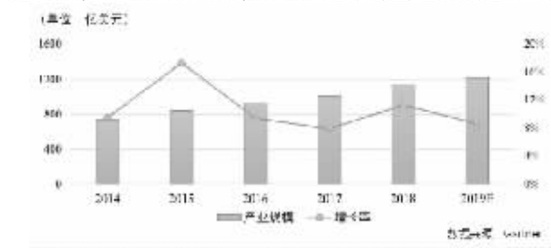
针对纯软件产品,产品的交付过程与软硬一体化产品存在差异。纯软件产品的交付包括两种方式:商务部通过邮件发送产品授权码给到客户,该情况下对方收到邮件即为产品签收;部分纯软件产品通过寄送光盘形式交付,该情况下客户收到并经确认后签署收货确认单据视为产品签收。订单审核、收入确认入账、开具发票及收款流程与软硬一体化产品相同。

(三)所处行业情况

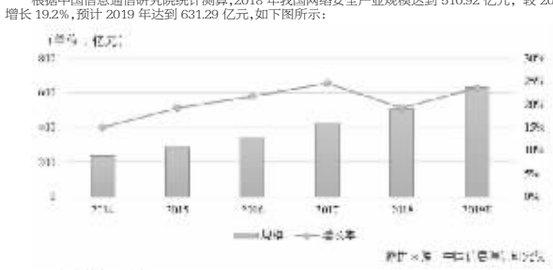
1.行业的发展阶段、基本特点、主要技术门槛

公司主营业务为网络安全核心软件产品的研究、开发、销售以及相关技术服务。根据国家统计局发布的《战略性新兴产业分类(2018)》,公司所处行业为“网络与信息安全软件开发”;根据中国证监会公布的《上市公司行业分类指引》(2012年修订),公司所处行业为“I65软件和信息技术服务业”;根据国家统计局发布的《国民经济行业分类》(GB/T4754-2017),公司所处行业为“软件和信息技术服务业”。根据公司主营业务的服务领域,公司属于网络安全行业。

根据中国信通院发布的《中国网络安全产业白皮书(2019年)》显示,2018年全球网络安全产业规模达到1119.88亿美元,预计2019年增长至1216.68亿美元。从增速上看,2018年全球网络安全产业增速为11.3%,创下自2016年以来的新高,2014-2019年全球网络安全产业规模及增速如下图所示:



根据中国信息通信研究院统计测算,2018年我国网络安全产业规模达到510.92亿元,较2017年增长19.2%,预计2019年达到631.29亿元,如下图所示:



(1)行业的发展阶段

① IPv6改造稳步推进,安全隐患亟待解决

根据中国信通院发布的《筑牢下一代互联网安全防线—IPv6网络安全白皮书》显示,截止2019年7月,全国已有12.78亿用户获得IPv6地址,其中,LTE网络用户共11.29亿,固定网络用户1.49亿,相比2018年初增长超过10倍,我国主要互联网应用活跃用户数已达2.01亿,网络基础设施IPv6升级改造基本完成,应用基础设施已具备IPv6服务能力。随着IPv6网络开始投入使用,IPv6网络攻击数量急剧增加,2019年上半年共监测发现超过9万起IPv6网络攻击,截止2019年7月,CVE漏洞库中已收录IPv6相关漏洞381条,覆盖系统漏洞、应用漏洞、硬件漏洞、协议漏洞等不同层面。

近年来,我国各政府部门立足自身职责分工,在政策方面频频发力,出台部门相关政策文件,同步强化各行业领域IPv6发展和安全工作部署,包括:工信部发布的《关于贯彻落实(推进互联网协议第六版(IPv6)规模部署行动计划)的通知》、《关于开展2019年IPv6网络就绪专项行动的通知》,国资委发布的《关于做好互联网协议第六版(IPv6)部署应用有关工作的通知》,广电总局发布的《广电有线网络IPv6规模部署及推进实施指南》,教育部发布的《教育部办公厅关于贯彻落实(推进互联网协议第六版(IPv6)规模部署行动计划)的通知》,央行发布的《关于金融行业贯彻(推进互联网协议第六版(IPv6)规模部署行动计划)的实施意见》。

随着问题凸显和政策落地,IPv6安全已成为网络安全的重点方向。

② 信息安全技术自主创新趋势明显

习近平主席在2016年发表重要讲话,提出“加快推进网络信息技术自主创新,朝着建设网络强国目标不懈努力”。2017年7月,国家互联网信息办公室起草《关键信息基础设施安全保护条例(征求意见稿)》,提出顶层设计、整体防护、统筹协调、分工负责的原则,充分发挥运营主体作用,社会各方积极参与,共同保护关键信息基础设施安全。信息安全产业作为信息安全技术、产品和服务提供者和实施者,承担着国家信息安全防御和保障的历史使命,发展壮大网络安全产业已经成为维护国家网络空间主权、安全和发展利益的战略选择。

近年来,国内信息安全厂商快速发展,依托本地布局的产品和研发团队,对用户需求理解更为透彻,对新需求的响应更为迅速,产品性价比更高,部分功能特性已超过国外厂商,但在高端产品市场的竞争力仍相对较弱。“十三五”时期,我国将大力实施网络强国战略,要求网络与信息安全有足够的保障手段和能力,通过切实推进自主可控和国产化替代,政策化培养和市场化发展双向结合,信息安全市场国产化脚步逐步加快。拥有自主可控的标准、技术、产品的信息安全厂商,将在为政府、行业服务的大背景下,充分应用包括云计算、大数据等技术,把握产业发展机遇,不断扩大市场份额,实现对国外信息安全产品的战略性替代,在核心应用领域和国内产业转型升级的变革中发挥重要作用,在国家网络信息安全领域中担当核心角色。

③ 5G正式商用,物联网安全和云安全市场高速增长

根据中国信通院发布的《物联网终端安全白皮书(2019年)》显示,2019年10月31日,工业和信息化部与中国电信、中国移动、中国联通、中国铁塔共同宣布启动5G商用服务,标志着我国正式进入5G商用时代,5G网络规模商用的快速来临,将极大促进蜂窝物联网终端规模化部署和应用。截至2019年,全球物联网设备连接数量达到110亿,据GSMA预测,2025年全球物联网终端连接数量将达到250亿,截至2019年第三季度,我国授权频段蜂窝物联网终端连接数量达到9.2亿,预计到2025年该数值有望突破19亿。针对“物联网终端安全能力较低”和“物联网卡难实现流量定向访问”的安全风险,可通过外在赋予安全能力的方式进行解决,外在赋予安全能力是指:在终端或网关中增加集成安全能力的模组、SDK(软件开发包)等套件,使得终端或网关具备接受、执行安全策略,以及上报访问行为数据等能力。

物联网安全事件从国家、社会、个人层出不穷,物联网设备、网络、应用面临严峻的安全挑战,物联网安全将成为万亿规模市场下的蓝海“潜力股”,2018年中国物联网安全市场规模达到88.2亿元,增速达到34.7%。

根据赛迪顾问股份有限公司发布的《2019中国网络安全发展白皮书》,2018年,中国云安全市场规模达到37.8亿元,增长率为44.8%。公有云的多租户共享场景将导致可信边界的弱化,威胁的增加,因此构建基于云的纵深防护体系成为应对公有云安全威胁的重要手段。私有云、行业云领域,众多厂商积极在云安全资源池、云工作负载保护平台等重点领域加速布局,公有云领域,公有云安全防护发展态势持续向好,领域生态初步成型。

④高级安全威胁需要多维分析和可视化呈现

在安全产品的发展过程中,将检测到的关键信息以日志等方式留存下来,以便满足检索和合规要求,这种技术架构存在了很长时间,但并未产生足够的价值。如今,安全事件变得越来越多样化,APT攻击常常由身份盗取、系统入侵、数据回传等多个环节构成,涉及到安全防护的多个环节,传统的单一层面安全分析无法解决问题。

在IDC发布的《中国安全管理平台(SOC)市场份额》中提出,在企业频频遭受多样化攻击的今天,恶意威胁的集中化、可视化和可分析化渐渐成为企业对安全投资的趋势。未来的安全管理分析,一定是基于多个维度综合进行的,方案需要覆盖到网络安全的主要板块例如边界安全、主机安全、流量安全等等方面,站在防御体系的宏观角度提供给用户统一的分析工具。另外,场景化数据分析方案已经流行开来,将采集到的数据按照不同的场景,例如潜在的泄密手段、舆论风险、员工离职倾向等,进行针对性的分析与呈现,让安全与用户的业务结合更紧密,从而体现出价值,而不仅仅是一种投资。

(2)基本特点

坚实的网络安全产业实力,是网络空间繁荣稳定、保障有力的前提和基础。习近平总书记在全国网络安全和信息化工作会议上强调,要树立正确的网络安全观,积极发展网络安全产业,做到关口前移,防患于未然,对新时代我国网络安全产业发展提出更高要求。

根据近年来,我国网络安全产业保持高速发展态势,2018年全球网络安全产业规模达到1119.88亿美元,预计2019年增长至1216.68亿美元,从增速上看,2018年全球网络安全产业增速为11.3%,创下自2016年以来的新高1,2018年我国网络安全产业规模达到510.92亿元,较2017年增长19.2%,预计2019年达到631.29亿元,从业企业近3000余家,产业体系日趋健全,技术新高度活跃,综合实力显著增强,为保障国家网络空间安全奠定了坚实的产业基础。

1数据来源:Gartner,Information Security and Risk Management,Worldwide,2017-2023

2数据来源:中国网络安全产业白皮书(2019年)

(3)主要技术门槛

公司所处网络安全行业属于技术密集型的高科技行业,公司技术具有较高的技术壁垒,主要体现在以下几方面:

① 核心技术研发难度大。公司目前所使用的核心技术,需要在设计之初就坚持技术路线,中途改造实现难度大。例如:对于硬件无关化技术,需要操作系统套件在设计之初就坚持在用户态实现,并且将对体系架构的依赖部分进行独立封装,才能实现。安全管理产品的核心技术安全合规路径可视化分析,需要计算和呈现全图上任一节点间的全部路径,相比地图类应用只处理最优的几条路径的模式,计算量和难度都更大。

② 核心技术需要长时间积累。公司目前所使用的核心技术,需要较长周期积累才能达到,而不能通过短期投入迅速实现。例如,对于硬件无关化技术,操作系统套件针对每一种体系结构和硬件形态的适配、稳定性测试和广泛应用,都需要一定时间周期;对于安全策略配置数据挖掘与分析技术,需要解析安全设备和网络设备的配置文件,所以对各类设备配置的解析工作需要较长的积累时间。

③ 核心技术不断迭代发展。公司产品涉及到互联网应用、新型安全威胁、新型信息网络等多个快速发展的因素,随着相关领域地不断发展,再加之众多客户不断提出新需求,推动公司核心技术不断迭代发展。因此,增大了技术追赶的难度,对行业内企业以及外部企业进入构成了较大壁垒。

④ 高端技术人才稀缺。公司处于网络安全产业链中的上游,产品核心技术的层次较高,需要聘请业内高端技术人才,这些人才在国内较为稀缺,在公司拥有较高的薪资待遇,而且一般与公司签订了保密协议与竞业禁止协议,使得行业内高端技术人才的获得难度较高,对行业内企业以及外部企业进入构成了较大壁垒。

2公司所处的行业地位分析及其变化情况

报告期内,公司专注于网络安全核心软件产品的研究、开发、销售以及相关技术服务,成功入选2019年度北京市知识产权试点单位名单。

公司为工信部网络安全威胁信息共享平台的技术支撑单位,2019年12月9日,安博通被授予工信部网络安全威胁信息共享平台合作单位奖牌,截至2019年10月31日,安博通向工信部威胁平台报送威胁信息113233条,在合作单位中排名第一。

公司投入开发的网络安全管理软件,可以作为业界各大产品与解决方案厂商网络安全态势感知解决方案的主要功能模块与数据引擎,该产品2016年和2017年连续两年入选工信部电信和互联网行业网络安全试点示范项目,2019年,攻击面可视化管理平台入选工信部网络安全技术应用试点示范项目,公司安全管理产品获得了中央网信办等行业管理部门与各行业用户的认可。在IDC发布的《IDC创新者:中国网络安全风险态势感知系统,2018》报告中,安博通作为五家企业之一入选。在第二届金融关键信息基础设施保护论坛上,安博通基于龙芯架构研发的国产自主软硬一体SORA安全管理平台荣获“补天奖”优秀产品之最具潜力奖。安博通流量安全可视平台获2019年度第一批(总第十批)北京市新技术新产品(服务)认证。

公司持续积累研发的网络安全系统平台已成为行业内多家大型厂商安全网关与安全管理类产品所广泛选用的软件平台,公司主要客户包括华为、新华三、星网锐捷、卫士通、启明星辰、360网神、任子行、绿盟科技、太极股份、荣之联、中国电信系统集成、迈普通信等知名产品与解决方案厂商。2019年,凭借强研发实力、高品质产品、快速的技术响应等多项综合实力,安博通全资子公司北京思普崚技术有限公司获得新华三集团“优秀供应商”的荣誉称号。

3报告期内新技术、新产业、新业态、新模式的发展情况和未来发展趋势

(1)IPv6大面积落地带动安全产品应用升级

2019年7月全国获取IPv6地址的用户数是2018年初的10倍,我国主要互联网应用活跃用户数已达2.01亿,网络基础设施IPv6升级改造基本完成,随着工信部、国资委、广电总局、教育部和央行出台推进IPv6部署应用的政策,2020年政府、运营商、金融和教育行业网络将进一步加速IPv6升级换代的速度。

在IPv6网络升级过程中,安全网关产品需要支撑IPv6和IPv4双协议栈、IPv6到IPv4隧道以及IPv6翻译等过渡业务,同时需要解决IPv6地址标识复杂性聚增带来的地址资源威胁和IPv6新特性引入的协议漏洞等安全问题。在IPv6网络中,互联网资产数量指数级增加,攻击暴露面急剧扩张,网络攻击方仅需在茫大的攻击面中发现一个或多个脆弱点作为突破口,即可发起针对性的攻击并向更深更广的范围渗透,为以缩小攻击暴露面的安全管理平台产品带来发展机遇。

(2)5G商用带动物联网边缘接入安全和流量元数据回溯需求

5G商用后,物联网终端数量爆炸式增长,物联网应用已经在制造、新零售、交通物流、政府、公共事业和医疗健康等行业大面积部署,但是物联网终端大量暴露在互联网上,且存在安全漏洞,导致终端被仿冒进而被当做跳板进行扩散攻击的情况频频发生,导致物联网应用失效,用户数据遭到窃取。而终端到管理业务平台的跨广域网传输网络部署范围广,构造和流量比较复杂,一旦发生网络攻击后很难定位溯源。

为了解决上述安全问题,需要在物联网边缘实现安全准入和安全防护,确保接入网络的终端已经在管理平台上合法注册,流量和协议符合规范且无安全威胁,同时需要在核心层实施传输网络的流量元数据存储措施,一旦出现业务质量和网络攻击问题,可以进行数据回溯及时定位和处置。

(3)应对高级威胁需要智能化、可视化、过程化的安全解决方案

根据腾讯安全威胁情报中心的研究,2019年全球披露的高级持续性威胁(APT)的总报告数量近500起,继续持续增长。国内政府、央企国企、科研单位和高校,尤其是涉及对外进出口、国防军工、外交等重点单位是APT攻击的重灾区。

传统的安全架构中,较多依赖特征匹配的模式。在这种模式中,防护设备需要先将某个攻击事件写入特征库,然后才能防御这个攻击,而且安全设备的特征库,数量是非常有限的,所以最大的问题在于滞后性和局限性,防护方永远落后于攻击方,对网络内资产的暴露面不清楚,产生大量事件日志但没有进行有价值的分析,导致对0day等高级威胁无能为力。

为了应对日益严重的高级持续性威胁,防守方也应该转向持续性过程安全防御,以下技术手段和产品将得到更多应用:

安全威胁情报:利用云存储、云更新、云推送解决局限性和滞后性问题

攻击面持续缩减:以可视化手段持续性分析和缩减网络的攻击暴露面

人工智能分析:对海量安全事件进行大数据建模和AI分析,基于特定攻击场景进行针对性威胁发现和防御

(4)信息安全技术自主创新产业链进一步成熟发展

“十三五”时期,信息安全市场的自主可控和国产化替代趋势非常明确,在2019年,不同体系架构的自主可控产业链均有重大进展。由飞腾CPU和银河麒麟OS联手打造的“PK体系”包括CPU、操作系统、BIOS、桥片等关键产品和数据库、开发工具、驱动等系统软件,在2019年推出了FT-2000+CPU,业界多家厂商推出了基于FT-2000+的产品。申威1621处理器是基于第三代“申威64”核心(增强版)的国产高性能多核处理器,目前已经实现量产,芯片产品涵盖超级计算机、服务器、桌面终端、嵌入式设备等,申威产业联盟的业务包括芯片设计、主板定制、整机制造、操作系统、应用软件等领域,已初步形成一个较完善的自主可控生态链。龙芯中科在2019年发布了龙芯新一代处理器架构产品龙芯3A4000/3B4000处理器,其中3A4000的性能是上一代产品的一倍,3B4000的性能是上一代产品的四倍以上。

从各生态体系的发展情况看,国产化产业链进一步成熟发展,在自主可控技术的关键技术和关键组件方面具备了更强的替代能力,性能大幅度提升,自主信息安全技术创新的网络安全产品将继续高速发展,真正做到保卫国家网络空间。

3公司主要会计数据和财务指标

3.1近3年的主要会计数据和财务指标

单位:元 币种:人民币

	2019年	2018年	本年比上年增减(%)	2017年
总资产	1,064,997,333.22	311,633,724.87	241.76	247,366,165.91
营业收入	248,731,759.62	195,346,548.76	27.33	150,756,321.61
归属于上市公司股东的净利润	73,771,975.96	61,549,570.52	19.86	36,047,465.23
归属于上市公司股东的扣除非经常性损益的净利润	68,990,205.17	60,003,247.62	14.98	34,581,655.25
归属于上市公司股东的净资产	999,665,911.12	255,418,127.27	291.38	203,948,811.25
经营活动产生的现金流量净额	22,940,105.08	18,031,979.95	27.22	19,342,122.05
基本每股收益(元/股)	1.77	1.60	10.63	0.97
稀释每股收益(元/股)	1.77	1.60	10.63	0.97
加权平均净资产收益率(%)	16.04	26.93	减少10.89个百分点	23.47
研发投入占营业收入的比例(%)	15.19	13.59	增加1.6个百分点	17.60

3.2报告期分季度的主要会计数据

单位:元 币种:人民币

	第一季度(1-3月份)	第二季度(4-6月份)	第三季度(7-9月份)	第四季度(10-12月份)
营业收入	29,206,057.73	42,451,498.16	55,605,152.58	121,469,051.15
归属于上市公司股东的净利润	-31,526.70	14,676,412.19	7,371,456.70	51,755,633.77
归属于上市公司股东的扣除非经常性损益后的净利润	-31,526.70	14,290,600.78	7,373,026.67	47,368,104.42
经营活动产生的现金流量净额	-6,787,529.27	10,239,387.32	6,640,288.29	12,847,958.74

季度数据与已披露定期报告数据差异说明

□适用 √/不适用

4股本及股东情况

4.1股东持股情况

单位:股

截止报告期末普通股股东总数(户)	7,402
年度报告披露日前上一月末的普通股股东总数(户)	6,377
截止报告期末表决权恢复的优先股股东总数(户)	-
年度报告披露日前上一月末表决权恢复的优先股股东总数(户)	-

前十名股东持股情况								
股东名称(全称)	报告期内增减	期末持股数量	比例(%)	持有有限售条件股份数量	包含转融通借出股份的限售股份数量	质押或冻结情况		股东性质
						股份状态	数量	
钟竹	0	13,460,000	26.30	13,460,000	13,460,000	无	0	境内自然人
石河子市峻盛股权投资合伙企业(有限合伙)	0	7,200,000	14.07	7,200,000	7,200,000	无	0	境内非国有法人
苏长君	0	3,240,000	6.33	3,240,000	3,240,000	无	0	境内自然人
武汉光谷烽火产业投资基金合伙企业(有限合伙)	0	3,100,000	6.06	3,100,000	3,100,000	无	0	境内非国有法人
深圳市和辉财富投资企业(有限合伙)	0	2,520,000	4.92	2,520,000	2,520,000	无	0	境内非国有法人
苏州厚扬景桥投资管理有限公司-宁波柳山保税港区厚扬天灏股权投资中心(有限合伙)	0	2,385,000	4.66	2,385,000	2,385,000	无	0	境内非国有法人
深圳市达晨财智创业投资管理有限公司-深圳市达晨财智二号股权投资企业(有限合伙)	0	1,800,000	3.52	1,800,000	1,800,000	无	0	境内非国有法人
深圳市磐鼎文井购基金合伙企业(有限合伙)	0	1,575,000	3.08	1,575,000	1,575,000	无	0	境内非国有法人
北京中金永合创业投资中心(有限合伙)	0	900,000	1.76	900,000	900,000	无	0	境内非国有法人
深圳市达晨财智创业投资管理有限公司-深圳市达晨创通股权投资企业(有限合伙)	0	500,000	0.98	500,000	500,000	无	0	境内非国有法人
上述股东关联关系或一致行动的说明	1、上述股东中深圳市达晨财智创业投资管理有限公司-深圳市达晨财智二号股权投资企业(有限合伙)与深圳市达晨财智创业投资管理有限公司-深圳市达晨创通股权投资企业(有限合伙)为关联方,公司未知其他股东之间是否存在关联关系或一致行动关系。2.公司未知涵通股股东之间是否存在关联关系或属于《上市公司股东持股变动信息披露管理办法》中规定的一致行动人。							
表决权恢复的优先股股东及持股数量的说明	无							

存托凭证持有人情况

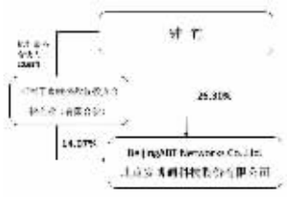
□适用√/不适用

4.2公司与控股股东之间的产权及控制关系的方框图

√适用 □不适用

4.3公司与实际控制人之间的产权及控制关系的方框图

√适用 □不适用



4.4报告期末公司优先股股东总数及前10名股东情况

□适用 √/不适用

5公司债券情况

□适用 √/不适用

三经营情况讨论与分析

1报告期内主要经营情况

报告期内,公司实现主营业务收入24,873.18万元,比2018年同期增长27.33%;归属于上市公司股东的净利润7,377.20万元,比2018年同期增长19.86%。

2面临终止上市的情况和原因

□适用 √/不适用

3公司对会计政策、会计估计变更原因及影响的分析说明

√适用 □不适用

根据财政部于2017年3月31日发布的《关于印发修订(企业会计准则第22号——金融工具确认和计量)的通知》《关于印发修订(企业会计准则第23号——金融资产转移)的通知》《关于印发修订(企业会计准则第24号——套期会计)的通知》及2017年5月2日发布的《关于印发修订(企业会计准则第37号——金融工具列报)的通知》,本公司自2019年1月1日起执行上述准则以下统称“新金融工具准则”),详情请见本年报第十一节财务报告五、重要会计政策及会计估计41、重要会计政策和会计估计的变更。

4公司对重大会计差错更正原因及影响的分析说明

□适用 √/不适用

5与上年度财务报告相比,对财务报表合并范围发生变化的,公司应当作出具体说明。

√/适用□不适用

子公司名称	注册地址	业务性质	持股比例(%)	取得方式
北京思普崚技术有限公司	北京市海淀区西北旺东路十号院东区15号楼A座301	销售及软件技术服务	100	设立
武汉思普崚技术有限公司	武汉东湖新技术开发区光谷大道308号光谷动力节能环保科技企业孵化器(加速器)一期11栋3层01室	销售及软件技术服务	100	设立
北京安博通云科技有限公司	北京市海淀区西北旺东路10号院东区15号楼-2至4层01地下一层B101	销售及软件技术服务	55	设立
湖北安博通科技有限公司	武汉市东湖新技术开发区光谷创业街特1栋1楼A11-122室	销售及软件技术服务	51	设立
广西安桂通信科技有限公司	南宁市高新区创新路23号4#楼B座1楼	销售及软件技术服务	51	设立
河南安博通软件科技有限公司	郑州市金水区金水路219号1号楼1单元18层1808号	销售及软件技术服务	51	设立
合肥安博通安网络安全有限公司	合肥市高新区黄山路605号民创中心119室	销售及软件技术服务	51	设立
天津睿邦安通技术有限公司	天津滨海高新区华苑产业区海泰西路18号南2-3042	销售及软件技术服务	100	收购
北京安博通金安科技有限公司	北京市西城区德胜门东宽闸路3号9号楼401室	科技推广和应用服务	100	设立

注:本期合并财务报表范围及其变化情况详见本节“八、合并范围的变更”和“九、在其他主体中的权益”。

证券代码:688168　证券简称:安博通　公告编号:2020-003

北京安博通科技股份有限公司 2019年度募集资金存放与使用情况专项报告

公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏,并对其内容的真实性、准确性和完整性依法承担法律责任。

一、募集资金基本情况

根据中国证券监督管理委员会(以下简称“中国证监会”)于2019年8月16日出具的《关于同意北京安博通科技股份有限公司首次公开发行股票注册的批复》(证监许可[2019]1513号)的核准,同意北京安博通科技股份有限公司(以下简称“公司”、“本公司”或“安博通”)向社会公开发行人民币普通股1,279.50万股,每股发行价格为人民币56.88元。截至2019年9月3日止,公司实际已发行人民币普通股1,279.50万股,募集资金总额人民币727,779,600.00元,扣除各项发行费用人民币57,303,792.11元,实际募集资金净额人民币670,475,807.89元。

上述募集资金于2019年9月3日到位,并经大信会计师事务所(特殊普通合伙)审验并出具了大信验字[2019]第27-00006号验资报告。

2019年度尚未使用募集资金进行项目投入,截止2019年12月31日,公司募集资金余额为83,393,390.48元。

二、募集资金管理情况

为了规范募集资金的管理和使用,保