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 是否存在公司占用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	夏振寤	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	010-57649050	010-57649050
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,为用户提供安全智能的一体化防护体系。

网络行为管理与审计产品提供对网络端统一管控功能,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、虚拟网络资源池化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网络流量可视化、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

公司目成立以来,坚持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、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维护联系过程中,将不同客户的需求统一交给产品部门,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。公司通过对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。公司按研发项目立项明细统计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,由各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供客户远程下载并记录使用数量,由公司提供序列号给客户激活使用,期间声明授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,专注于网络安全行业上游网络安全软件系统的提供。

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、交付地点及付款方式等相关事项。对此类项达成一致后,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,商务部根据市场情况决定是否接受客户的销售合同/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:一是通过互联网软件系统,客户通过互联网软件系统确认和报确认,商务部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,财务部据此编确认收入并入账;同时经总经理审批通过后,由商务部开具发票。商务部根据双方约定的合同期限,跟踪应收账款回款情况。

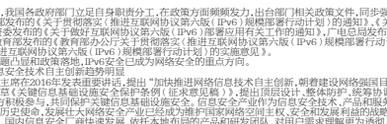
针对纯软件产品,产品的交付过程与软硬一体化产品存在差异。纯软件产品的交付包括两种方式:商务部通过邮件发送产品授权码给到客户,该情况下对方收到邮件后即完成产品的交付;商务部也可以通过密钥光盘形式交付,该情况下客户收到并经确认后签收货确认单据视为产品签收。订单审核、收入确认入账、开具发票及收款流程与软硬一体产品相同。

(三) 所处行业情况

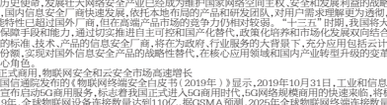
1.行业的发展阶段

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“网络与信息安全产业”,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“65 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安全能力提升,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适配用户数已达201亿,网络基础设施IPv6升级改造基本完成,应用基础设施全面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37万起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,我国各政府部门交足自身职责分工,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迎势明显

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《关于加强网络安全保护条例(征求意见稿)》,提出顶层设计、整体协护、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,国内信息安全产业快速发展,依托本地市场的竞争力和相对较强、一定程度的政策支持,国内信息安全产业在技术、产品和服务提供方面,在某些领域已经具备了一定的国际竞争力,并在自主研发的基础上,通过切实推进自主可控和国产化替代,政策化将养和市场化发展双向结合,信息安全市场国产化趋势逐步加快。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4G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,我国投资网络蜂窝物联网终端连接数量达到3.2亿,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监测”的安全风险,可通过外在硬子安全能力的方式进行弥补,外在硬子在终端或网关中增加集成安全能力的模组 .SDK(软件开发包)等软件,使得终端或网关具备接受、执行安全策略,以及上报动向行为数据等能力。

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98.2亿元,增速达到34.7%。

根据赛迪顾问股份有限公司发布的《2019网络信息安全发展白皮书》,2019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,公有云安全的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,将检测到的网络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DDC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、可视化和可分析化都亟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,并在对威胁的全面检测的基础上,另外,还需要能够提供协同响应能力,将采集到的数据及时反馈给安全设备,以便进行防御的动作,并进行对威胁的分析与呈现,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

随着网络安全产业实力,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,和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1119亿美元,预计2019年增长至1216亿美元,从增速上看,2018年全球网络安全产业增速为11.3%,自下自2016年以来的新高,2018年我国网络安全产业规模达到510亿元,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、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、交付地点及付款方式等相关事项。对此类项达成一致后,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,商务部根据市场情况决定是否接受客户的销售合同/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:一是通过互联网软件系统,客户通过互联网软件系统确认和报确认,商务部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,财务部据此编确认收入并入账;同时经总经理审批通过后,由商务部开具发票。商务部根据双方约定的合同期限,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后即完成产品的交付;商务部也可以通过密钥光盘形式交付,该情况下客户收到并经确认后签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产品相同。

(三) 所处行业情况

1.行业的发展阶段

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“网络与信息安全产业”,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“65 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安全能力提升,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适配用户数已达201亿,网络基础设施IPv6升级改造基本完成,应用基础设施全面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37万起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,我国各政府部门交足自身职责分工,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迎势明显

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《关于加强网络安全保护条例(征求意见稿)》,提出顶层设计、整体协护、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,国内信息安全产业快速发展,依托本地市场的竞争力和相对较强、一定程度的政策支持,国内信息安全产业在技术、产品和服务提供方面,在某些领域已经具备了一定的国际竞争力,并在自主研发的基础上,通过切实推进自主可控和国产化替代,政策化将养和市场化发展双向结合,信息安全市场国产化趋势逐步加快。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4G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,我国投资网络蜂窝物联网终端连接数量达到3.2亿,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监测”的安全风险,可通过外在硬子安全能力的方式进行弥补,外在硬子在终端或网关中增加集成安全能力的模组 .SDK(软件开发包)等软件,使得终端或网关具备接受、执行安全策略,以及上报动向行为数据等能力。

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98.2亿元,增速达到34.7%。

根据赛迪顾问股份有限公司发布的《2019网络信息安全发展白皮书》,2019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,公有云安全的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,将检测到的网络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DDC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、可视化和可分析化都亟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,并在对威胁的全面检测的基础上,另外,还需要能够提供协同响应能力,将采集到的数据及时反馈给安全设备,以便进行防御的动作,并进行对威胁的分析与呈现,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

随着网络安全产业实力,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,和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1119亿美元,预计2019年增长至1216亿美元,从增速上看,2018年全球网络安全产业增速为11.3%,自下自2016年以来的新高,2018年我国网络安全产业规模达到510亿元,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、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、交付地点及付款方式等相关事项。对此类项达成一致后,双方签署合作合同,公司承担向客户转让商品的主要责任。

② 核心技术更迭快、技术壁垒高、专业性强的标准化产品,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、交付地点及付款方式等相关事项。对此类项达成一致后,双方签署合作合同,公司承担向客户转让商品的主要责任。

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,需要熟谙业内高端技术人才,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,在增强被授予下属单位的威胁信息共享平台合作单位资格,截至2019年10月31日,安博通网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,该由面对电信行业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兴通讯、奇安信、天融信、绿盟等行业管理厂商了中兴通讯的《中国新者·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SOR入安全管理平台荣获“补天奖”优秀产品之最具潜力奖。安博通成量安全可视平台获2019年度第一届(总第十届)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、大极股份、荣之联、中国电信系统集成、迅雷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,安博通会资子公司北京思普睿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月全国互联网应用适配用户数达201亿,IPv6地址的用户数达10亿,我国主要互联网应用适配用户数已达 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、教育部相关部门出台推进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升级换代的进程。

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地址标识复杂性带来的地址管理问题、IPv6网络中,互联网资产数量剧增及暴露面急剧扩张,网络攻击方式需在匿名方式下进行的攻击面扩大等问题,在IPv6网络中,互联网资产数量剧增及暴露面急剧扩张,网络攻击方式需在匿名方式下进行的攻击面扩大等问题,对用户需求理解能力透明,对需求的响应更为迅速,产品价价比更高,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。“十二五”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,政策化将养和市场化发展双向结合,信息安全市场国产化趋势逐步加快。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。

(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、虚拟网络资源池化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网络流量可视化、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

公司目成立以来,坚持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、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维护联系过程中,将不同客户的需求统一交给产品部门,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。公司通过对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