



面向大型企业信息安全建设的 虚拟化威胁感知技术

徐影¹, 吴钊², 李祉岐³

(1. 北京联合大学, 北京 100101; 2. 国网信息通信产业集团有限公司, 北京 102200;
3. 北京国电通网络技术有限公司, 北京 100070)

摘要: 面对信息化建设进程的快速推进, 如何有效实现风险防控, 建立先进实用、安全可靠的信息安全保障体系, 是大型企业都要面临的严峻考验。分析了大型企业在信息化建设中面临的各种安全风险和信息安全防护工作的主要特性, 提出了具有实践意义的信息安全防护体系建设思路。分析了大型企业信息安全建设虚拟化环境面临的威胁, 设计出一种虚拟化安全威胁感知系统, 该系统由威胁情报平台、本地检测系统和数据分析平台组成。

关键词: 信息安全; 安全风险; 安全防护; 威胁感知

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016310

Perception technology of virtual threat for large enterprise's information security construction

XU Ying¹, WU Zhao², LI Zhiqi³

1. Beijing Union University, Beijing 100101, China

2. State Grid Information & Telecommunication Group Co., Ltd., Beijing 102200, China

3. Beijing Guodiantong Network Technical Co., Ltd., Beijing 100070, China

Abstract: Facing with the rapid development of the progress of the information construction, how to effectively achieve the risk prevention and control, in order to build the advanced, practical, safe and reliable information security system, is a severe test to every large enterprise. By analyzing the main characteristics of various security risks and the information security protection, which are faced by large enterprises in the information construction, the practical ideas for the construction of information security system was put forward. Furthermore, the threat that faced by the large enterprise's virtual environment of information security construction was analyzed, a virtual threat perception system was designed, which consists of threat intelligence platform, the local detection system and data analysis platform.

Key words: information security, security risk, security protection, threat perception



1 引言

网络与信息安全风险随着信息化建设的加速推进和发展而增高,企业必须高度重视网络与信息安全体系的建设。习近平总书记于2016年4月19日在网络安全和信息化工作座谈会^[1]上明确指出:网络安全和信息化是相辅相成的,安全是发展的前提,发展是安全的保障,安全和发展要同步推进。大型企业作为国家经济的主体,信息安全工作十分重要且繁杂,既要考虑信息安全对企业管理、运营以及社会、经济效应的影响,又要考虑企业肩负的法律与社会责任乃至国家安全责任。随着云计算、大数据、物联网、移动应用(简称“云大物移”)等新技术的迅猛发展,新技术的快速应用与落后的企业传统信息安全管理之间的矛盾日益凸显。大型企业如何建立有效的信息安全保障体系、形成基于自身特点的防护策略、有效提升信息安全防护与管理水平、加强网络安全防御和威慑能力,是当前大型企业信息安全工作面临的首要任务。

2 大型企业信息安全建设现状

在国家“积极防御、综合防范”的信息安全战略引领下,企业对信息安全给予高度重视,已将信息安全建设视

为企业发展战略的重要组成部分,正在陆续加快信息安全自身能力建设。但总体来看,多数企业的信息安全保障体系建设仍有待完善。大型企业信息安全建设宜从以下几方面入手。

2.1 信息安全威胁源

企业要从自身的社会和经济价值出发,全面分析企业面临的安全威胁,既要明确威胁源的等级,也要结合企业安全责任来分析威胁。企业必须全面梳理信息安全需要保护什么、为什么保护和如何保护等关键问题,明确对现实中的安全威胁和未来可能的安全风险的预期。企业可能的威胁源如图1所示。

大型企业拥有大量商业及企业机密,容易成为恶意竞争对手和黑客集团的攻击对象,生产经营中的大量有价值的信息数据,可能成为不法分子和黑客获取利益的目标。部分企业涉及国家科研、国防等重要领域,承担国家重要基础设施建设,拥有重要的国家机密,容易被敌对势力及政治团体选中作为主要的攻击对象。敏感信息泄露、重要数据被破坏、业务系统被非法控制、商业信誉遭恶意言论攻击,任意一种情况都将造成重大社会影响,甚至危及国家安全。威胁源分类及其带来的安全威胁见表1。

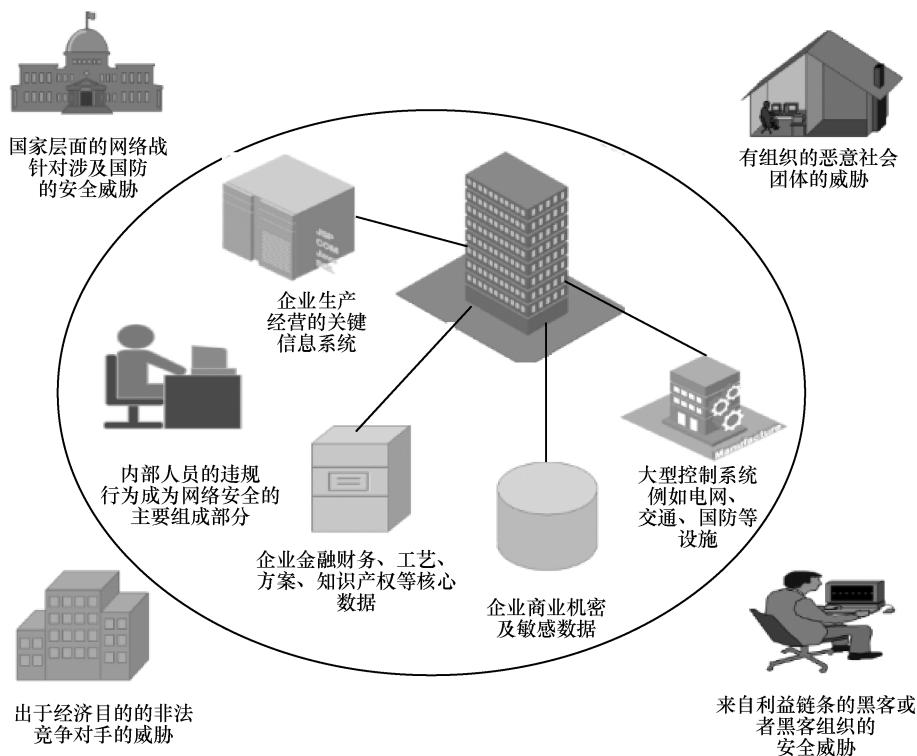


图1 企业可能的威胁源

表 1 威胁源及其安全威胁

威胁源分类	安全威胁
政府、国家	军工、电力、铁路、金融、石油等支柱行业肩负国家经济命脉、关系国家安全和稳定,成为敌对势力“网络战”的目标
竞争对手	出于企业社会经济效益考虑,多数情况下针对企业攻击都在试图盗取企业的敏感信息,如客户数据、商业机密、配方、流程等。在特定情况下,其目标是进入关键系统或者使业务流程中断,给目标企业造成经济损失
社会组织	大型企业社会参与度广,汇集了大量的个人数据,特别是电信、金融、电力等,利用于这些信息获利已形成了成熟的产业链条,严重威胁个人隐私安全
黑客组织	随着 APT(advanced persistent threat,高级持续性威胁)攻击等最新攻击技术的发展,黑客组织采用反复渗透、巧妙植入、长期潜伏、精确打击等先进的攻击手段,精确选择攻击目标进行持续性的攻击,能绕开传统的安全防护机制
内部人员	研究表明,安全事件 70%以上都是由内部人员的违规行为造成的,可能造成机密文件、核心数据泄露,系统运行存在安全隐患

2.2 企业的自身特性

信息安全工作不能是盲目的、通用的建设工作。信息安全工作首先应该从企业自身特性入手,做好常规安全措施的同时,深挖企业安全薄弱点进行加固、加强,有点有面,才能保证信息安全工作的效果。大型企业与信息建设紧密相关的特性如下。

(1)资产规模大、分布广泛

大到企业生产经营、金融财务,小到企业知识产权、生产工艺、流程配方、方案图纸、客户资源及各种数据,都是企业长期积累下来的财富,关系到企业的生存与发展,是企业安全防护的重要保护对象。这些庞大的无形及有形资产广泛分布于企业的各个系统中,给信息安全防护带来更高的要求。

(2)网络覆盖广、需求复杂

企业网络和系统结构复杂、交互需求多样。很多集团类大型企业信息网络由总公司、本地下属工厂、子公司独立建成局域网,并形成各自的应用系统,总公司整合分散的局域网构成总公司级局域网,并形成总公司级的应用系统,如 ERP(enterprise resource planning,企业资源计划)系统和 OA(office automation,办公自动化)系统,再发展到利用专线将跨省市的外地子公司及下属工厂的局域网相连,

形成了复杂的网络环境及系统结构。有些大型企业各地内部相关系统与其他单位系统有相互访问的需求,部分大型企业既承担着民用设施的建设,又涉及军工设备的制造,这些特点都是企业信息安全应重点关注的问题,也给信息安全工作提出了不同的防护需求。

(3)安全管理难、风险较高

大型企业人员众多、信息安全管理涉及面广、管理工作相对繁杂。安全培训工作的全面开展、员工安全防护意识培养、办公系统与生产系统安全的区分管理、应用系统安全的统一建设、安全机制建设漏洞与安全保障措施执行力度检查,都是企业信息安全工作的重要部分,如果有一个环节被不法集团利用,就容易形成“木桶效应”,会给原有严密规划的纵深安全防御体系造成漏洞。

2.3 信息化安全的建设过程

企业的信息安全工作应该融入自身信息化建设过程中。IT 技术产品的应用不仅要符合企业架构与流程的变化,也要充分考虑信息安全的问题,加大信息化建设中“人”的安全意识、IT 技术产品的安全性^[2],在信息化建设规划的同时,开展信息安全防护研究和配套安全设施的建设。信息系统与设备的安全风险如图 2 所示。

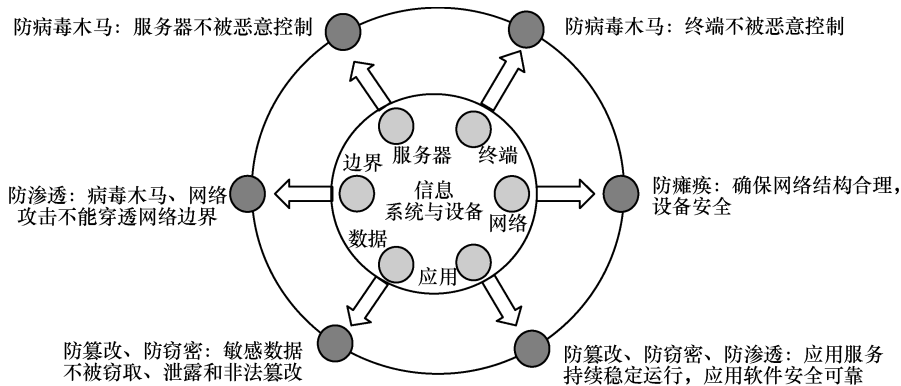


图 2 信息系统与设备的安全风险



目前多数大型企业在业务系统和办公终端的管理建设中,并未建立全面统一的漏洞状况监控系统,也未建立终端补丁统一管理、补丁统一分发的安全控制系统,使得系统及终端在补丁及时更新、漏洞全面修复等方面不具备条件,企业内部信息安全由于漏洞修复不及时、不全面而陷于大量的威胁之中。

3 企业虚拟化环境威胁梳理

3.1 传统防护手段面临失效

高级持续性威胁 (APT) 是一种可以绕过各种传统安全检测防护措施,通过精心伪装、定点攻击、长期潜伏、持续渗透^[9]等方式,伺机窃取网络信息系统核心资料和各类情报的攻击方式。事实证明,传统安全设备已经无法抵御复杂、隐蔽的 APT 攻击。

几乎所有被曝光的 APT 攻击都是以入侵者的全面成功而结束,在这些已公开的 APT 攻击中,传统安全设备的防御体系均被轻易绕过而失去防御能力。在某些 APT 攻击的案例(如震网攻击、夜龙攻击)中,传统安全防御设备甚至在长达数年的持续攻击中毫无察觉,传统安全设备无法抵御网络攻击的核武器——APT。

传统安全防御体系的框架一般包括:接入控制、安全隔离、边界检测/防御、终端防御、网络审计、访问控制等,所涉及的安全产品包括:防火墙、IDS/IPS、杀毒软件、桌面管理软件、网络审计、双因素认证 token 等。

从传统安全防御体系的设备和产品可以看出,这些产品遍布网络 2~7 层,其中,与 APT 攻击相关的 7 层设备主要是 IDS、IPS、审计,而负责 7 层检测的 IDS、IPS 采用经典的 CIDE 检测模型,该模型最核心的思想就是依靠攻击特征库的模式匹配完成对攻击行为的检测。反观 APT 攻击,其采用的攻击手法和技术都是未知漏洞 (Oday)、未知恶意代码等未知行为,在这种情况下,依靠已知特征、已知行为模式进行检测的 IDS、IPS 在无法预知攻击特征、攻击行为模式的情况下,理论上就已无法检测 APT 攻击。

(1) 多变的攻击手段

这些由黑色产业链或国家驱动的 APT 攻击通常都具备强大的攻击手段和技术,且手法多样,在一次攻击过程中经常采用多种手段和技术,包括社会工程学攻击、Oday 漏洞利用、免杀木马、定制化工具、逃逸技术等,寻找内部安全薄弱环节,所以可以屡屡得手,很难被发现。

(2) 攻击隐蔽性强

在大部分 APT 攻击中,攻击者针对不同的攻击目标会采用不同的策略,并在攻击前有针对性地进行信息收集,准备特定的攻击工具,攻击发起的整个过程时间可长可短,少则数小时,多则潜伏数月、数年,由于这些攻击均会使用高级免杀技术以逃避传统安全设备的特征检测,因此隐蔽性极强。

(3) 攻击目标明确

APT 攻击往往具有明确的攻击目的,如窃取有价值的信息、破坏重要系统等,由于传统防护手段很难对此类攻击有防护效果,一旦受到攻击,其对企业 and 单位所造成的危害也是直接而巨大的。

在安全形势极不乐观的环境下,如何摆脱传统思路,寻求精确的 APT 攻击检测方法是亟待解决的问题。

3.2 免杀木马无法检测

木马 (trojan), 也称木马病毒,是通过特定的程序 (木马程序) 来控制另一台计算机的软件。木马通常有两个可执行程序:控制端和被控制端。木马程序是目前比较流行的病毒文件,与一般的病毒不同,它不会自我繁殖,也并不“刻意”地去感染其他文件,它通过将自身进行伪装吸引用户下载执行,向施种木马者提供打开被种主机的门户,使施种者可以任意毁坏、窃取被种者的文件,甚至远程操控被种主机。在 APT 攻击中,通常使用“免杀木马”,这类木马会利用加冷门壳、加花指令、改程序入口点、修改内存特征码等免杀技巧来避免自身被杀毒软件查杀。

3.3 大量内网数据无法有效利用

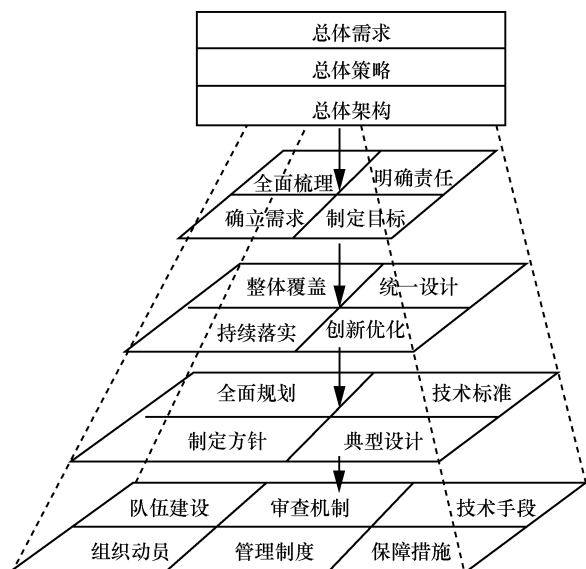
APT 攻击通常都会在内网的各个角落留下蛛丝马迹,真相往往隐藏在网络的流量中。传统的安全事件分析思路是遍历各个安全设备的告警日志,尝试找出其中的关联关系。但根据上文的分析,由于 APT 攻击的隐蔽性和特殊性,传统安全设备通常都无法对 APT 攻击的各个阶段进行有效的检测,也就无法产生相应的告警,安全人员花费大量精力进行告警日志分析往往都是徒劳无功。如果采用全流量采集的思路,一方面是存储不方便,每天产生的全流量数据会占用过多的存储空间,组织通常没有足够的资源来支撑长时间的存储;另一方面是全流量数据包含了结构化数据、非结构化数据,涵盖了视频、图片、文本等多种格式,无法直接进行格式化检索,安全人员也就无法从海量的数据中找到有价值的信息。

因此,如何以恰当的方式长时间保存对安全分析有价

值的流量数据,是检测、回溯 APT 攻击必须解决的问题。

4 企业信息安全建设思路

大型企业的信息安全建设,首先应明确安全需求,制定企业总体安全防护策略。在总体策略的指导下,开展针对企业自身特性的安全防护体系建设,规划和设计总体防护结构,形成信息安全防护技术典型设计。在坚持和落实企业防护策略的基础上,逐步标准化技术要求、细化技术措施,最终形成人员、管理、技术的有效措施。大型企业安全工作建设思路如图 3 所示。



4.1 制定与落实企业总体防护策略

企业要深入分析梳理各级工作内容、明确方针策略和防护原则、构建安全防护总体策略。通过安全管理、人员组织、工作机制、标准规范、技术措施、运行管控等手段规范指导企业的信息安全建设工作,确保信息安全策略的一致性,在具体方案中坚持策略。公司各级单位要根据总体防护策略并结合自身实际,在遵循主体内容不变的基础上开展信息安全防护工作。

企业的防护策略要有稳定性和前瞻性,要结合技术和业务发展趋势,一方面需针对“云大物移”等新技术的引入,从宏观上对技术应用带来的风险进行综合考虑,对在建项目在规划阶段就展开安全防护研究和运行管控;另一方面不断提升自身认知,保障企业的安全方针和策略要在一段时期内持续有效,形成规划总体防护策略的演进线路,以适应或引领企业信息安全的发展潮流。

4.2 规划与设计总体防护结构

企业要明确内部各级单位各类场景的防护需求、规划和设计总体防护结构。总体防护结构要遵循国家有关信息安全法规、标准和行业监管要求^[4],坚持“规划定级、标准设计、全面建设、有效防护”的工作原则,有效衔接自身安全防护体系和国家防护体系,形成企业内部、外部有效协同和整体联动机制。

企业总体防护结构要充分结合自身特点展开设计,要实现管理技术与技术体系的融合,有效支撑业务安全发展。企业在总体防护结构的框架下,继承和巩固已有的成果,逐步细化完善各级保护标准,开展新技术、新制度的创新应用。

4.3 构建全生命周期的管理机制

在健全信息安全规章制度、加强安全管理体系、安全技术体系、安全运维体系的基础上,企业应构建全生命周期的管理机制。规范风险控制方法和工作流程,强化信息安全风险识别、风险评估、措施制定、过程控制和应急处置等工作,从信息化管理机制、规章制度、标准规范、设备设施、软件质量、人员管理等多方面出发,将信息安全贯穿信息系统规划、设计、研发、建设、施工、运维到销毁等生命周期的全过程和信息化全部领域,形成有效的企业信息安全体系,融入信息化管理各项工作中。全生命周期管理机制的构建见表 2。

同时,企业应健全和完善信息化考核评价管理体系,建立信息化建设与运行过程情况的有效描述模型,帮助企业识别相关技术与管理的不足,逐步改善信息化过程,达到持续改进的目标。

4.4 提高信息安全动员和协调能力

在信息安全技术威胁复杂多变的新形势下,企业需提高信息安全协调动员能力,确保发生重大安全事件的追查处理能力。从企业组织机构设置、人员队伍建设和管理机制方面进行建设提升,提高企业的信息安全动员能力,形成分工明确、专业处置、快速响应的信息安全管理队伍;建设网络安全事件应急处置工作机制,做到积极预防、及时发现、快速响应、确保恢复。

企业需提高各个业务部门的安全协作意识,确保防护策略能够有效贯彻和落实到各个业务部门,确保系统建设从规划设计、上线运行到下线报废的各个环节都在安全部门的有效监管下进行,安全部门在防护方案、安全测评、安全运行和应急响应等各个方面提供支撑服务,以形成高效的安全管控机制。



表 2 全生命周期管理机制的构建

阶段	工作	具体保障措施
规划	方案论证 方案审核	实行严格的方案论证及方案审核,确立规范的信息安全技术标准,保障技术方案的合理设计,各级部门应依据企业信息安全总体规划和总体策略,制定业务应用系统安全规划
设计、研发	安全体系 测评体系	建立合理的安全体系和测评体系,健全信息安全管理机制,形成规范的安全技术标准,建立内部安全测试机制,完善内部安全测试手段
建设、施工	安全检测 上线测评 安全评估	建立安全有效的管控机制,做好安全评估、安全检测、上线测评工作,加强人员队伍管理;协同研发单位、信息运维机构共同制定安全防护实施方案,并开展安全防护建设
运维	督查机制 运维安全 应急机制	制定严格的督查机制,加强人员队伍的建设和建设,建立专业可靠的信息安全运维团队,确保运维环节的有效监督。提升企业安全动员能力,形成分工明确、专业处置、快速项目的信息安全管理控体系
销毁	检测验证督查	规范系统检测验证流程,强化督查考核机制,提高人员安全风险意识,确保数据安全转存、数据安全销毁及数据保密管理

5 虚拟化安全威胁感知系统架构设计

5.1 虚拟化安全威胁感知系统的组成

(1) 威胁情报平台

为保障虚拟化网络的安全,避免重要机密和信息被窃,需要建立基于大数据分析的威胁情报平台。基于大数据分析的威胁情报^[9]平台,可通过对互联网上的海量数据进行深度挖掘,从而有效发现 APT 攻击,生成威胁情报。

(2) 本地检测平台

传统防病毒网关和杀毒软件对于免杀木马的查杀无能为力,为有效检测网内的免杀木马,应该建立本地检测平台。

本地检测平台可对 APT 攻击的核心环节——恶意代码植入进行检测,与传统的基于恶意代码特征匹配的检测方法不同,基于多引擎沙箱的本地检测平台采用的多引擎沙箱方法可以对未知的恶意代码进行有效检测,可以避免因为无法提前获得未知恶意代码特征而漏检的问题,在无需提前预知恶意代码样本的情况下,仍然可以对恶意代码样本进行有效的检测,因为免杀木马是 APT 攻击的核心步骤,因此对未知恶意代码样本的有效检测,可以有效解决 APT 攻击过程中的检测问题。

(3) 数据分析平台

为有效发现网络内部的安全问题,必然需要对网络内部的流量信息和终端的日志信息进行抓取,这必然带来如何在海量数据中快速搜索有用信息的问题。为了解决这个问题,应该建立基于搜索技术的数据分析平台。基于搜索技术的数据分析平台可对本地抓取的海量数据进行快速检索从而进行高效分析,对内网的攻击行为进行历史回溯。

5.2 本地信息处理

本地信息采集是通过虚拟化安全威胁感知系统传感

器^[6](采集设备)对网络流量进行解码,还原出真实流量提取网络层、传输层和应用层的头部信息,甚至是重要负载信息,这些信息将通过加密通道传送到分析平台进行统一处理。

分析平台承担对所有数据进行存储、预处理和检索的工作。由于传统关系型数据库在面对大量数据存储时经常出现性能不足的问题导致查询相关数据缓慢,因此分析平台底层的数据检索模块需要采用分布式计算和搜索引擎技术对所有数据进行处理,通过建立多台设备的集群以保证存储空间和计算能力的供应。

5.3 本地沙箱检测

虚拟化安全威胁感知系统通过检测器对文件进行高级威胁检测,威胁器可以接收还原自采集器的大量 PE 和非 PE 文件,使用静态检测、动态检测等一系列无签名检测方式发现传统安全设备无法发现的高级威胁,并将威胁相关情况提供给安全管理人员。检测器上的相关告警也可发送至分析平台,实现告警的统一管理和后续分析。

5.4 云端威胁情报

5.4.1 大数据分析

虚拟化安全威胁感知系统依托 IP、DNS、URL、文件黑白名单信誉数据库^[7],对互联网上活跃的任何一次攻击进行记录。DNS 库、样本库以及主防库需要定期维护更新,因为要发现未知威胁需要真实网络环境下的大量数据支撑。

5.4.2 数据处理

通过 DNS 解析记录、样本信息、文件行为日志等内容,对全网抓取数据、可视化的分析数据以及其他多个维度的数据进行关联分析和历史检索,依赖于虚拟化安全威胁感知系统发现 APT 攻击组织信息,并不断地跟踪相关

信息,依赖于海量数据对攻击背景做出准确的判定。

5.4.3 确认未知威胁

所有大数据分析出的未知威胁都通过专业的人员进行人工干预,做到精细分析,确认攻击手段、攻击对象以及攻击的目的,通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌,包括程序形态、不同编码风格和不同攻击原理的同源木马程序、恶意服务器(C&C)等,通过全貌特征“跟踪”攻击者,持续地发现未知威胁,最终确保发现的未知威胁的准确性。

5.4.4 情报交付

为了将云端的攻击发现成果传递到管理侧,虚拟化安全威胁感知系统将所有与攻击相关的信息(如攻击团体、恶意域名、受害者 IP 地址、恶意文件 MD5 等)进行汇总,按照标准格式封装成威胁情报,并通过加密通道推送到管理侧的威胁感知系统。作为系统整个方案的核心内容,威胁情报承担了连接互联网信息和本地信息的重要作用,为 APT 事件在管理侧的最终定位提供了数据线索和定位依据。

6 某大型企业的信息安全建设实践

某大型企业在“十一五”期间,遵循国家信息安全战略,提出了信息安全保障体系的建设需求,制定了信息安全防护体系总体策略,按照“双网双机、分区分域、等级防护、多层防御”的总体思路,建成了以“三道防线”为基础的总体布防结构,初步建设了信息安全等级保护纵深防护体系,如图 4 所示。

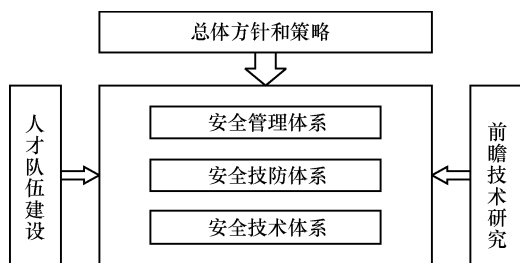


图 4 某大型企业的信息安全体系

在“十二五”期间,通过信息安全顶层设计,确立安全方针和策略,形成多层次、系统性的规范文件,并在规范文件的指导下,建立信息安全管理、技防体系和技术体系。

安全管理和各类防护措施进一步细化,持续完善管理与制度保障体系,建立有效管理机制,推进自主可控安全建设,开展人才队伍管理与建设,从人才技术水平提升、技术装备提升两方面提升信息安全专业队伍水平。

展望“十三五”,该企业充分考虑新技术安全需求与挑战,提出了“可管可控、精准防护、可视可信、智能防护”的安全防护理念,强化了网络与信息安全技术检查、网络与信息安全内控、网络与信息安全基础防护和信息安全动员等能力建设,对信息安全主动防御体系进行优化提升,为新技术应用安全防护提供技术路线,保障信息化战略的创新演进,为信息安全防护体系创新提供了新动力。

7 结束语

新型国家信息安全形势下,针对大型企业信息化建设进程中存在的风险、特性和实际诉求结合当前虚拟化网络环境设计出一种基于大数据分析的虚拟化安全威胁感知系统。详细阐述了企业信息安全工作需要考虑和关注的问题,提出了大型企业信息安全建设的总体思路,并列出了某大型企业的信息安全建设实践。大型企业信息安全防护,只有通过持续不断地创新建设,不断优化和完善企业信息化管理体系,遵守符合各种业务发展需要及国家行业政策的要求,才能使企业的信息安全保障能力和风险管控能力不断提升到更高的水平。

参考文献:

- [1] 习近平总书记在网络安全和信息化工作座谈会上的重要讲话[EB/OL]. (2016-04-26)[2016-08-01]. http://news.xinhuanet.com/newmedia/2016-04/26/c_135312437.htm.
President Xi's important speech at the forum on network security and information technology [EB/OL]. (2016-04-26)[2016-08-01]. http://news.xinhuanet.com/newmedia/2016-04/26/c_135312437.htm.
- [2] 互联网时代的企业安全发展趋势专题研究报告[EB/OL]. (2013-09-24)[2016-08-01]. <http://www.newhua.com/2013/0924/233390.shtml>.
Research on the development trend of enterprise security in internet era[EB/OL]. (2013-09-24)[2016-08-01]. <http://www.newhua.com/2013/0924/233390.shtml>.
- [3] 闫世杰, 陈永刚, 刘鹏, 等. 云计算中虚拟机计算环境安全防护方案[J]. 通信学报, 2015, 11(1): 15-36.
YAN S J, XU Y G, LIU P, et al. Security protection scheme of computing environment of virtual machine in cloud computing[J]. Journal of Communications, 2015, 11(1): 15-36.
- [4] 中国电子信息产业发展研究院. 信息安全产业发展白皮书(2015 版)[R]. [S.l.:s.n.], 2015.
China Electronic Information Industry Development Research Institute. The white book of the development of information security industry(2015 edition)[R]. [S.l.:s.n.], 2015.



- [5] DENI C. Acronis releases vmProtect 6 data protection for virtual machines[J]. ProQuest, 2013, 11(3): 1-23.
- [6] TIM G. Start-up offers rootkit protection, partitions virtual machines[J]. ProQuest, 2013, 5(2): 24-44.
- [7] SHI J, YANG Y, TANG C. Hardware assisted hypervisor introspection[J]. Springerplus, 2016, 5(1): 1-23.

[作者简介]



徐影(1974-),女,北京联合大学电信实训基地讲师,主要研究方向为计算机技术、信息安全。



吴钊(1972-),男,国网信息通信产业集团有限公司高级工程师,主要研究方向为信息化规划、IT治理、信息安全。



李祉岐(1986-),男,北京国电通网络技术有限公司工程师,主要研究方向为电力云计算系统架构、云安全。