主机安全强化策略在复杂网络环境中的应用

陈　强
浙江省发展信息安全测评技术有限公司　浙江杭州　310000

摘　要：在信息化与网络化深度融合的当今时代，主机身为网络体系里的核心节点，是承担数据、运行应用以及控制资源的关键载体，随着网络结构朝着复杂化发展以及攻击手段趋向智能化，主机所面临的安全威胁变得越发多样且隐蔽，以往传统的被动防御举措已很难契合复杂网络环境下的安全要求。主机安全强化作为网络安全防护体系的关键构成部分，借助系统配置优化、访问控制加强、漏洞修补管理、入侵检测以及行为监测等方式来提升主机的整体安全韧性，本文依据复杂网络环境的安全特性，全面分析主机安全威胁的演变走向与攻击路径，深入探讨主机安全强化的关键技术策略以及实际应用途径。

关键词：主机安全；安全强化；网络防御；漏洞管理；行为监测

引言

在数字经济跟智能网络快速发展的情形下，主机安全成为网络安全体系里的基础部分以及关键防线，主机身为数据的载体以及运算核心，它的安全状况直接决定整个信息系统的防御能力，不过复杂网络环境下的安全形势越发严峻，网络攻击的组织化、隐蔽化、链式化特点持续提高，攻击者借助多点渗透、权限提升、远程控制等办法，利用系统漏洞、配置缺陷以及人为失误，对主机进行长期潜伏以及定向破坏。一旦主机被攻陷，数据泄露、业务中断甚至系统瘫痪等严重后果就难以避免，传统防护体系以防火墙和杀毒软件为代表，主要依靠外围防御和静态检测机制，但是它对零日攻击、内生威胁和多阶段攻击的防御能力有限，复杂网络环境的安全防护需要转向以主机为中心的纵深安全机制，主机安全强化策略的提出正是应对这一挑战的有效途径，凭借系统性、安全性与智能化相结合的方式，从底层操作系统到应用层安全控制，构建多维协同防御结构。本文探讨主机安全强化的理论基础与实践路径，分析其在复杂网络环境中的应用价值与优化方向，为网络安全防御体系的建设提供参考。

一、复杂网络环境下主机面临的安全威胁与防护挑战

1.网络攻击的多样化与智能化趋势

随着信息化程度持续提升，网络攻击的形态以及手段正在经历从“单点入侵”朝着“多阶段、链式攻击”的演变过程，以往传统的病毒传播或者木马注入已然被更为复杂的攻击链所替代，攻击者大多时候依照“信息侦察—漏洞利用—持久驻留—数据窃取—痕迹清除”这样的路径来开展长期潜伏式攻击。在这个过程当中，攻击工具呈现出高度模块化、自动化的特点，形成了完整的“黑产产业链”，当下最具代表性的攻击类型覆盖勒索病毒、挖矿木马、供应链攻击以及远程控制工具滥用等。

勒索病毒借助加密主机文件并索要赎金这种手段来获取非法收益，已然成为企业所面临的主要威胁之一，挖矿木马利用主机资源开展加密货币挖掘活动，致使系统性能出现下降情况，同时能耗也随之增加，而更具隐蔽特性的APT攻击，是依靠将自身伪装成合法通信或者更新程序的形式，持续不断地对目标系统进行渗透。

人工智能和机器学习技术被引入后，攻击模式有了智能化的趋势，攻击者借助人工智能来自动识别漏洞、生成社会工程钓鱼邮件以及伪装入侵行为，使得攻击路径更具随机性与隐蔽性，部分攻击还可以在防御系统的学习过程中对模型进行“反训练”，导致出现误判和防护失效的情况，这让传统基于特征匹配或黑名单机制的安全防御手段渐渐失去效用，实时检测和溯源分析面临着更大挑战。

2.系统漏洞与配置缺陷的安全隐患

在复杂网络环境里，主机操作系统以及各类应用程序大多时候进行更新，随着功能不断扩展且兼容性有所提高，新的安全漏洞也不可避免地被引入进来，攻击者

作者简介：陈强（1995——），男，汉，浙江杭州，本科，主要从事计算机网络安全方面的研究工作。

借助自动化漏洞扫描和利用工具，像Metasploit、Cobalt Strike等，针对目标系统展开批量化探测。一旦察觉到存在未修补的漏洞，便可凭借缓冲区溢出、代码注入或者权限提升等手段达成渗透控制。

除了漏洞利用之外，系统配置方面存在的不当情况同样也是主机安全当中容易出现问题的隐患所在，常见的问题包含了弱口令设置、远程桌面端口暴露、默认账户没有禁用、访问权限划分不够合理以及日志审计存在缺失等，根据相关研究统计得出，大概有70%的主机安全事件是和配置错误或者管理疏漏直接关联的。这样的一个比例体现出了传统运维模式里面“以功能优先、忽视安全”所存在的长期弊端。

在云计算以及虚拟化的环境当中，这样的问题显得格外突出，共享资源池要是出现配置错误的情况，就有可能致使多租户之间出现越权访问的现象，要是容器与镜像管理方面做得不妥当，那么就可能引发供应链层面的安全风险，说构建规范化的漏洞修补机制以及自动化配置检测系统，是主机安全防护的基础保障。

现代安全运维体系需要从以往的“被动响应”模式转变为“主动防御”模式，借助漏洞生命周期管理、自动补丁分发以及安全基线审计等一系列手段，把潜在的威胁在攻击的前端就进行遏制。

3.内生威胁与人为因素的复杂性

除了来自外部的攻击之外，内部人员出现的不当行为已然成为对主机安全构成威胁的关键因素，这里所说的“内生威胁”包含误操作、因疏忽大意而产生的问题以及恶意破坏这三种形式，那些拥有系统访问权限的内部员工或者外包人员，一旦出现违规操作的情况或者账户凭证被盗取，那么攻击者就可较为轻易地绕过传统的外围防护体系，直接接触到核心系统以及敏感数据。

在“远程办公”以及“云化运维”变得日益普遍的情形下，企业的访问边界被极大程度地模糊了，传统依靠固定IP与静态权限的身份认证机制很难有效分辨合法行为与异常行为，比如说，攻击者可借助社交工程或者钓鱼邮件来窃取管理员凭证，接着借助合法的远程通道登录系统，达成对核心主机的完全控制。

内部安全意识薄弱也是安全风险的关键来源，部分员工缺少基本的网络安全培训，容易被钓鱼网站、恶意附件或社会工程攻击诱导，据安全机构统计，超过60%的企业安全事件都和人为因素直接有关。

要构建全员参与的主机安全文化，借助定期开展的安全教育、遵循访问权限最小化原则也就是Least Privilege以及多因素身份认证即MFA机制，来提高整体防御水准，把用户行为分析技术也就是UBA与零信任安全框架即Zero Trust相结合，达成基于行为特征的动态风险识别，实时监测异常操作与权限滥用情况，从根本上减小人为风险带来的影响。

二、主机安全强化的核心理念与体系构建

1.最小权限原则与访问控制强化

主机安全强化的首要原则乃是最小权限原则，此原则规定系统里的每个用户、进程以及应用仅有完成自身任务所需的最低限度权限，以此从源头上降低高权限被滥用以及横向渗透的风险，举例而言，普通用户对于系统关键目录、注册表以及网络端口的访问应当给予限制，而管理员权限则需要借助分级授权以及动态审批机制来实施严格管控。借助细粒度的访问控制列表以及基于角色的访问控制，可达成权限依据需求进行分配以及动态调整的目的，将多因素身份验证与会话审计机制相结合，可切实防止凭证泄露以及非法登录的情况发生。

另外要引入零信任架构理念，把身份验证、访问授权以及行为监控融入主机安全体系里，保证“永不默认信任、持续验证授权”，系统在每次访问请求时都要重新校验用户身份、设备安全状态以及环境可信度，构建动态、闭环的访问控制体系。

2.多层防御体系与安全策略协同

主机安全防护需依照纵深防御即Defense in Depth原则来构建，以此形成有多个层次、覆盖全面范围的安全屏障，于操作系统层面，借助关闭那些并非必要的服务以及端口，强化内核安全模块像SELinux或者AppArmor，严格落实补丁管理以及系统日志审计等方式，减少潜在的攻击面。在网络层面布置主机防火墙也就是Host Firewall、入侵检测与防御系统即HIDS/IPS，同时结合端口扫描防护以及流量白名单策略，以此防止外部的渗透行为以及异常通信情况的发生。

在应用安全方面，要借助代码审计、输入过滤以及沙箱隔离等方式来防止程序执行漏洞被利用，于数据保护方面，则需实施加密存储、数字签名以及完整性校验，以此防止数据出现泄露与篡改的情况，要构建跨层联动机制，一旦任一防护层检测到异常，就能自动触发响应策略，像访问阻断、日志上报或者进程隔离等。

借助统一的安全策略中心，达成主机防护、日志分析以及应急响应的协同运行，最终塑造出动态感知、主动防御且智能响应的综合安全体系，让主机于复杂网络威胁环境里维持持续防御能力与运行稳定性。

三、主机安全强化的关键技术与应用策略

1.漏洞管理与系统加固技术

漏洞管理属于主机安全强化里的基础部分，利用自动化漏洞扫描工具定时检测系统以及应用的安全缺陷，并且结合补丁管理系统达成及时修复，可降低被攻击的风险，对于操作系统层面，要采用安全基线加固标准，统一配置策略，涉及密码复杂度、账户锁定策略、日志审计以及安全策略模板化管理。企业可以引入CIS或者国标等级保护规范，达成主机加固的制度化与标准化。

2.入侵检测与行为分析技术

传统的入侵检测系统主要依靠静态特征匹配来开展工作，然而其在对未知攻击的识别能力方面存在欠缺，基于人工智能的主机入侵检测以及行为分析技术逐渐成为了新的防护发展趋势，借助采集主机系统调用、日志行为以及进程特征等信息，运用机器学习算法构建行为模型，可实现对异常活动的实时识别。比如说，当系统监测到进程频繁地访问敏感文件或者尝试进行提权操作时，便可以触发自动警报以及阻断机制，行为分析还可与大数据安全平台进行联动，达成跨主机关联分析，提前识别出潜在威胁。

3.安全审计与追踪溯源机制

在复杂的网络环境里，安全事件的可追溯性显得格外关键，主机安全强化需要覆盖全面的安全审计机制，针对系统操作、文件变更以及登录行为等展开记录并且进行加密存储，借助集中式日志管理以及链路追踪技术，可迅速定位攻击路径以及责任主体，联合区块链存证技术可达成关键安全日志的防篡改存储，提升取证的可信度，为安全事件分析以及司法追责提供相应依据。

四、主机安全强化在复杂网络中的实践应用

1.企业级主机安全防护体系构建

在企业信息系统里，主机安全强化要和网络安全、应用安全、数据安全共同构建起统一防护框架，企业可借助部署主机防护平台达成集中管理，囊括漏洞修复、配置合规、行为监测以及安全基线控制等功能，借助自动化策略分发与远程管理机制，提高安全运维效率，要联合SOC安全运营中心，达成安全事件的统一监测与应急响应。

2.云计算环境下的主机安全强化实践

云主机作为复杂网络里的关键构成部分，它的安全强化面临着全新挑战，云环境当中资源共享以及虚拟化特性致使安全边界变得更为模糊，对于云主机而言，要采用虚拟化安全加固策略，像是启用虚拟防火墙、监控虚拟机之间的通信、隔离高风险实例等，借助云安全管理平台也就是CSPM来达成安全策略自动化检测，以此保障云主机配置符合规定。并且要利用云端威胁情报系统达成动态防御，依据威胁等级自动调整安全策略，提升主机防护的智能化程度。

结束语

复杂网络环境下的主机安全防护属于一项有系统性以及动态化特点的工程，随着攻击技术持续演变，主机安全强化的重点已不再仅仅是修补漏洞以及防御攻击，而更需要重视体系化建设以及智能化演进，本文围绕威胁特征、技术策略以及实践应用这三个方面对主机安全强化的核心路径展开了探讨。研究显示，主机安全防护应当构建在最小权限原则、纵深防御结构以及行为智能分析的基础之上，达成从静态防御朝着动态响应的转型，未来的发展方向覆盖：其一，构建自主可控的主机安全框架，以此提升核心技术的独立性，其二，深入推进人工智能与安全管理的融合，达成主动预测以及自适应防护，其三，完善安全治理体系，把主机安全纳入组织整体安全战略。依靠不断优化技术体系以及管理机制，方可在复杂网络环境里有效维护主机安全的稳定性与可靠性，为数字化社会的可持续发展给予坚实支撑。

参考文献

[1]青藤发布千载·全栈信创主机安全产品[J].中国信息安全，2023，(12)：92.

[2]刘浩，周灿，鲍坤夫，等.面向混合云的主机安全纵深防御架构设计与实践[C]//中国计算机学会.第38次全国计算机安全学术交流会论文集.奇安信科技集团股份有限公司，2023：211-214.DOI：10.26914/c.cnkihy.2023.035939.

[3]朱小琴，杨勇，李文辉.数据协同关联分析的主机安全管理防护系统[J].信息技术，2023，(07)：136-141.DOI：10.13274/j.cnki.hdzj.2023.07.024.

[4]张中超，韩斌，邓永敏，等.主机安全加固技术在电力行业的应用[J].自动化应用，2023，64(06)：45-47.

[5]丁知逾.资产评估业务系统主机安全问题研究[J].网络安全和信息化，2022，(11)：1-3.

[6]费禹.基于EDR的高校内网终端主机安全防护体系[J].现代信息科技，2022，6(14)：51-53+57.DOI：10.19850/j.cnki.2096-4706.2022.014.012.