**基于攻击视角完善信息安全弹性防御体系的思考**

中国人民银行金融信息中心  吕毅

目录

[**基于攻击视角完善信息安全弹性防御体系的思考** 1](#_Toc519452006)

[**行业现状：** 2](#_Toc519452007)

[**基于攻击者视角构建纵深弹性自适应网络安全防御生态** 2](#_Toc519452008)

[**1.基于攻击链路径构建纵深防御体系** 2](#_Toc519452009)

[**主要原则有三：** 2](#_Toc519452010)

[**2.强韧性、异构、自适应能力弹性及强韧性。** 3](#_Toc519452011)

[**防守异构是基于完全信息静态博弈中攻守平衡原理。** 4](#_Toc519452012)

[**基于此，应构建多样化异构防御体系。** 4](#_Toc519452013)

[**构建自适应防御体系及运营体系。** 4](#_Toc519452014)

[**3.信息交换，构建安全生态圈** 4](#_Toc519452015)

[**基于比较优势理论，开展信息交换。** 5](#_Toc519452016)

[**基于威胁情报及态势开展升维防御。** 5](#_Toc519452017)

[**有必要关注的几点** 5](#_Toc519452018)

[**4.稳健原则开展安全运营，开展威胁情报共享** 7](#_Toc519452019)

**行业现状：**

基于对信息风险的理解，参照ISO27000标准族，遵循GB20274《信息系统安全保障评估框架》、等级保护标准族及银行业各类信息安全综合规范及监管要求，目前银行业基本建立较完善安全保障体系，夯实安全生产三道防线，其落地在于安全运营能力的增强。体现在从构建纵深安全防御体系、持续改进安全能力建设、风险应急响应常态化、内外部威胁情报使用持续进化，信息安全运营体系具备自我学习，弹性增强及自适应能力。

随着云安全、大数据的发展及银行科技转型加快，安全保障更多作为一种服务为科技及业务赋能，提供更好用户体验。基于攻击链模型优化防御体系（防守），根据钻石模型开展攻击者分析（溯源），综合攻击链及钻石模型开展情报驱动的主动防御（升维防御）。在防御体系进化中，根据组织人财物锚定信息安全防御能力滑动象限（SANS）范围，有所为有所不为，实现成本和回报的适度安全。最后，在安全运营中辅助开展毒性测试以增强组织防御的强韧性以至于自适应升级，保证安全生态体系保持自适应进化。

**基于攻击者视角构建纵深弹性自适应网络安全防御生态**

**1.基于攻击链路径构建纵深防御体系**

攻击链模型源自美国军方，将攻击成功行为分为7步，每一步的打断均可有效阻止一次攻击行为，类似不完全信息动态博弈（精炼贝叶斯均衡），就算被攻击后的亡羊补牢，也为时未晚。

为此，纵深防御从攻击链的七步对应出来，按照时间维度，从事前监测、事中遏制及阻断、事后跟踪及恢复三个方面进行阐述。

**主要原则有三：**

一是在攻击链的不同阶段，部署不同防护策略，以实现互补；二是基于OSI模型，在网络、应用分别部署以展现；三是同一防护手段，在不同物理位置防护效果不一样，譬如对于SQL注入，在WAF层面、WEB日志、RASP和SQL数据库审计层面效果差距很大。

基于此，基于攻击视角，结合威胁情报的纵深防御架构应该实现的架构见表所示。

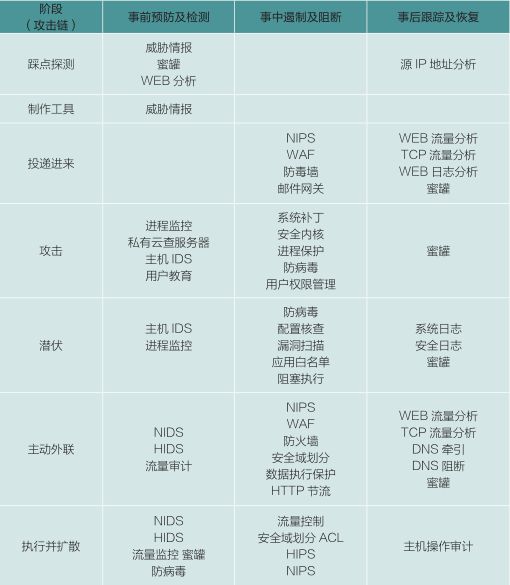


表  纵深防御从攻击链及其应对策略

该架构是在传统架构上的延展，在上云和大数据以后，理念通用。上云后从成本及效能的角度，防御方法偏向于分布式架构中的安全域隔离划分，通过业务数据流驱动进行建模及关联分析，安全以服务及组件的形式提供给业务（租户），基于大数据开展用户标签及画像，通过用户行为开展适度的安全预测。

**2.强韧性、异构、自适应能力弹性及强韧性。**

基于医学的毒性测试机制及牛顿机械论的反馈机制，构建系统弹性及强韧性。系统风险指威胁利用系统脆弱性的可能性。威胁对应外界刺激，刺激看剂量。16世纪毒理学帕拉塞尔苏斯（Paracelsus）毒物兴奋效应(hormesis)的名言“剂量决定毒物”，即所有物质都是有毒的，只和剂量大小有关。脆弱看自身，《反脆弱》作者纳西姆·尼古拉斯·塔勒布将系统刺激应变分为脆弱性、强韧性、反脆弱性三类。脆弱性可以理解为固化架构，在遇到风险时无法变通应对，造成信息安全事件被动应对，四处救火，修修补补。强韧性指信息系统在遇到外界变动时具备冗余性，在单点被攻破的情况下仍能保持正常运转。而反脆弱则说明信息系统安全水平在外界刺激下增强，具备免疫力并自我进化，例如人类婴儿水痘防疫或佛学的涅槃重生。为此，信息系统应不定期开展低微剂量毒性测试（自测评及渗透测试），根据系统反馈开展定点修补；定期开展众测及业务连续性（BCP）测试，通过中等剂量外界刺激，促进安全架构重构及进化，具备强韧性和弹性。

**防守异构是基于完全信息静态博弈中攻守平衡原理。**

基于攻防双方力量的博弈，就算防御方力量大于攻击方并且相同条件下占优，攻防双方无论怎么排兵布阵，按最优方式排列，获胜的概率也是相等，均为50%，从战局看，是典型的弱势攻击方战胜强势防守方。

**基于此，应构建多样化异构防御体系。**

同时，分散后对管理效能提出了更高的要求，采取分散策略的前提是：有效分散，即保证分散后单独防守能力不低于分散前，否则会适得其反。

**构建自适应防御体系及运营体系。**

自适应安全架构（ASA）是由Gartner在2014年提出的安全体系，类似于PDCA的戴明环理念，强调以持续监控和分析为核心，将防御、检测、响应、预测四个方面结合起来，自适应不同系统基础形态和业务系统变化，能够持续的自我进化，自我调整来适应不断变化的攻击类型。

太阳底下没有新鲜事。ASA架构也趋同于基于时间轴响应的PDR模型（保护、检测、响应），但ASA优点是加入了对威胁情报的引入和使用。

**3.信息交换，构建安全生态圈**

习近平总书记在今年4月的网信工作会议中指出“在信息时代，网络安全是整体的而不是割裂的，是动态的而不是静态的，是开放的而不是封闭的，是相对的而不是绝对的，是共同的而不是孤立的”。凯文·凯利(KK)在《失控》中也多次强调生态圈与自适应进化概念，对信息安全来说，亦提倡构建安全生态圈。

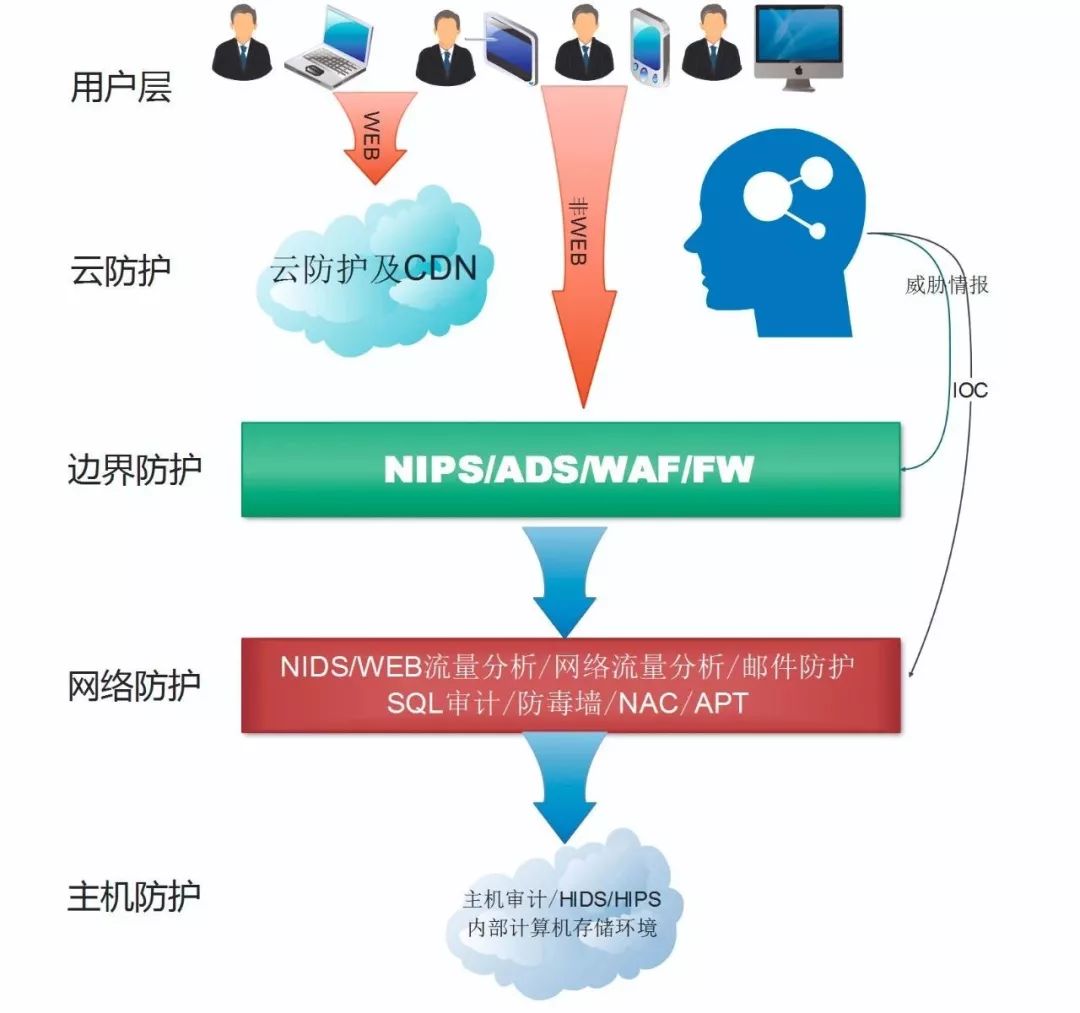


 图  基于攻击者视角纵深防御架构

**基于比较优势理论，开展信息交换。**

古典经济学家李嘉图比较优势理论对比于斯密的绝对优势，即使信息交换的弱方各类要素禀异均占劣势，通过交换的强弱各方也可以获得超额收益。其落地体现为，各企业信息安全机构以及行业主管部门联合起来，开展威胁情报及信息专项交换，获得效率的增量提升。

**基于威胁情报及态势开展升维防御。**

防守方可以利用外部威胁情报造成信息不对称，对攻击方开展升维防御。同时，通过对自身情报的采用和外部情报消费，对传统防护设备如邮箱防护、防火墙、IPS、WAF进行赋能。

**有必要关注的几点**

“不谋全局者，不足谋一隅”。在做好安全技术和管理日常运行和储备的同时，需要具备前瞻性，以战略眼光，全局角度跳出安全看安全，倡导适度安全，还需要注意以下几点。

1. **知己知彼，百战不殆，梳理好资产**

随着业务的发展，特别是云计算平台及移动互联网时代的到来，快速原型、精益开发、敏捷开发部署，灰度发布。如不掌握详尽的资产信息，一是家底不清，已发生问题无法快速应对定位；二是外部威胁情报到来后无法快速判断，造成精力分散和过度应对。

**实际工作中，至少应掌握两类资产**

一是系统资产，包括但不限于网络拓扑结构、业务逻辑架构、物理部署位置、系统数据流等，同时对资产的不光有内部报送，也应辅助扫描机外部探测；二是管理资产，包括但不限于组织架构图，研发、运维、供应链信息，保障及监管单位流程。

**2.具备四个意识，防范创造性失灵**

**安全要和企业的整体战略、规模、成本结合起来，实事求是做安全，不能过度安全导致影响业务。**

具有核心意识，向单位业务核心业务靠拢，保障核心业务；具有大局意识，从整体的信息系统发展角度出发而非只从狭隘的安全角度出发；具备看齐意识，向行业、国内、国际的顶端安全理念看齐；具有政治意识，保证安全工作和信息化工作的合规和合法。

**防御系统出现创造性，系统性失灵，类似明斯基时刻，整体失效。**

凯文凯利（KK）在《失控》中将各种质量控制手段和反馈手段综合起来，可证明随着各种防控手段的综合应用，综合防御能力会出现1+1>2的情况。但根据热力学第二定律，宇宙的熵会随着时间的流逝而增加，随着复杂度的增加，由有序向无序，最终进入热寂（创造性失灵并且无法定位故障点），这是大概率的系统性风险或明斯基时刻。

**3.信息安主动迎接云、大数据和区块链等新技术**

就像互联网的出现，电商颠覆了传统业态一样，云和大数据出现也对传统安全防护提出了挑战。安全体系应主动变革，从基础设施（IAAS）、操作系统（PAAS）、软件服务（SAAS）三个层面主动设计应对。

**云安全的实现路径首先开展统一的访问控制4A，统一入口。**

其次开展业务层的隔离与追踪取证，基于业务逻辑开展软件定义安全，软件定义边界和微隔离。最后开展数据安全治理，在业务隔离的基础上开展追踪取证，对数据打标并在边界进行控制。

**云安全时代的到来会带来一种变革，业务的入口更集中，安全相对来说也变的更集中，访问控制单点突破后，造成的损失几何级上升。**但云安全时代的好处在于将力量分散的安全能力进行聚合，能力越大，责任就越多，对安全人员提出了更高的技术要求，知识升级和安全理念的更新。

**4.稳健原则开展安全运营，开展威胁情报共享**

稳健（Prudent）原则开展安全运营，银行业属于风险厌恶型，运营稳健涵盖谨慎、负责、勤勉和有能力。为此遵循适度谨慎（DueCare）和适度勤勉（DueDeligeou）准则开展运营设计。在安全管理设计上逻辑严密，体系架构合理并可实现，在安全运营上要注意留存记录及证据，以便回查。这样，事件调查处置中，以证明制度和运营的合理性，尽职尽责，避免造成人为重大疏忽，也是对单位资产和从业者的保护。

信息安全工作由于其不直接产生经济效应，在信息系统中处于相对弱势，安全界自称背锅侠，“没出事情的时候没什么用，出了事情就证明真没什么用，重保三宝，预案、检讨和辞呈”。正因如此，从业者跟更应该团结起来，开展信息交换，实现非对称打击或者防御。在第6届银行业数据中心联系会上，银行业形成共识，通过银行业威胁情报及安全事件信息共享，构建联防联治态势体系，用开放、共享、共赢的方法来主动应对外部攻击，提升信息安全防御维度。

此外，不仅向内做好用户风险警示，更要向管理层和监管层就安全风险预期达成一致，设立合理安全目标，实现适度安全。

**安全的目标不是消灭所有的风险，是基于成本和效率的考量，将信息安全风险控制在管理层“可接受”范围内。**