

简译版

## 进攻性思维对于有效的网络防御至关重要

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	An offensive mindset is crucial for effective cyber defense		
原文作者	约翰·德西蒙 (John DeSimone)	原文发布日期	2022 年 5 月 11 日
作者简介	约翰·德西蒙是 Raytheon Intelligence & Space 公司的网络安全、情报和服务总裁。		
原文发布单位	Help Net Security		
原文出处	<a href="https://www.helpnetsecurity.com/2022/05/11/offensive-mindset-cyber-defense/">https://www.helpnetsecurity.com/2022/05/11/offensive-mindset-cyber-defense/</a>		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
摘要	随着网络犯罪的日益复杂，威胁环境也在不断演变。在这种情况下，保持进攻性思维对于保护组织免受企业 and 国家层面的攻击至关重要。组织应立即采取行动，改变招聘和培训员工的方式，像黑客一样思考，并同步推进进攻和防御培训。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

## 进攻性思维对于有效的网络防御至关重要

约翰·德西蒙

2022 年 5 月 11 日

随着勒索软件攻击的不断增加和网络犯罪分子的日益老练,联邦政府在网络安全方面实施了更加主动的“零信任架构”战略,以降低网络攻击对数字基础设施带来的风险。他们还还为各机构设定了具体的安全目标,以快速检测、隔离和响应威胁。此外,工业控制系统网络安全计划也采用了零信任方法。该计划旨在促进相关技术和系统的部署,为供水基础设施提供网络威胁可见性、指标、检测和告警。

进攻性思维是确保最佳网络防御的关键。在制定基于进攻性网络模型的防御策略时,组织需要考虑三个重要内容:(1) 重新考虑人才招聘问题;(2) 像黑客一样思考;(3) 进攻培训与防御培训相结合。

### 重新考虑人才招聘问题

根据 ISACA 的《2022 年网络安全状况》报告,63%的受访组织存在网络安全职位空缺问题,比 2021 年增加了 8 个百分点。随着人才缺乏问题的逐年加剧,企业应考虑聘用那些寻求更多职业(特别是在网络行业)成长和转变的人才。归根结底,网络安全是一个“问题和解决方案都层出不穷”的创造性领域,因此聘用“以新方式看待问题和渴望学习”的人才,比只盯着学位或经验更有价值。

这意味着企业应制定招聘计划,聘用可能不完全符合其网络标准的人才,并为他们提供培训,帮助他们掌握职位所需的技能。此外,为现有员工提供新的机会也很重要——企业应鼓励员工内部流动,将技能从一个部门转移到另一个部门。企业可以用这些方法来吸引网络人才,让他们相信会一直有成长空间。

### 像黑客一样思考

威胁情报是培养进攻性思维的关键部分,主动的网络安全审计是阻止网络攻击的最佳方案之一。为了对网络安全战略实施正确的更改,企业需要充分了解现有的网络漏洞。

这可以通过几种不同的策略来实现,包括渗透测试和漏洞扫描等。渗透测试是指测试人

员故意侵入企业网络以识别系统的弱点；而漏洞扫描是指执行自动化测试，以寻找潜在安全漏洞。这两种策略都能够帮助企业更好地了解黑客的想法和潜在攻击方式。在适当的情况下，企业可以考虑雇用前黑客，这是因为前黑客们具备识别系统弱点的能力，是一种非常有用的资产。许多前黑客很乐意接受橄榄枝，这是因为作为渗透测试人员/红队成员，他们不仅可以合法地寻找系统漏洞，还能够帮助企业提高安全性。

## 进攻培训与防御培训相结合

目前，联邦政府正在推动零信任策略，以更好地保护系统。但是，我们还需要认识到，所有部门都需要磨练进攻能力，以确保其防御方法的有效性。

私营部门或关键基础设施公司的网络安全专家，应采取“主动防御”（active defense）方法，在威胁破坏系统之前就能主动地加以识别和遏制。这就需要了解黑客是如何思考的，以便在威胁进入系统之前及时发现它们。

那些在网络领域寻求合法合规职业的人员，通常被教导如何保护网络。但是，除非他们知道如何渗透各个安全层，否则就无法像攻击者一样思考。为员工提供进攻性网络培训，有助于他们掌握安全技能和专业知識，成为最佳网络防御者。未来，“进攻培训和防御培训相结合”一定会成为标准实践。

“使用进攻性策略入侵系统”的经验，能够激发员工对防御方式的思考，这与了解攻击者的方法和动机一样有价值。

随着网络犯罪的日益复杂，威胁环境也在不断演变。在这种情况下，保持进攻性思维对于保护组织免受企业和国家层面的攻击至关重要。组织应立即采取行动，改变招聘和培训员工的方式，像黑客一样思考，并同步推进进攻和防御培训。

## 安天简介

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势，打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足客户对于包括终端杀毒、终端防护 (EPP)、终端检测与响应 (EDR)、云工作安全防护 (CWPP) 等系统安全层面需求；整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力；基于流量产品探海有效应对客户对于网络威胁检测与响应 (NDR) 和网络流量分析 (NTA) 的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到高级威胁 (APT) 的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

安天为网信主管部门、军队、部委、保密行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，已连续七届蝉联国家级网络安全应急支撑单位。安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑。

目前，安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过三十亿部智能终端设备提供了安全检测能力，已经成为“国民级”引擎。

安天已发展成为以哈尔滨为总部基地，建有六地研发中心、两个控股子公司，参与一个国家工程实验室建设，拥有两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在地多设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：

<http://www.avlsec.com>