简译版

成功进行网络防御的六个方法

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	The 6 steps to a successful cyber defense		
原文作者	丹尼尔·斯派塞（Daniel Spicer）	**原文发布日期**	2022 年 5 月 4 日
作者简介	丹尼尔·斯派塞是 Ivanti 公司的首席安全官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/05/04/map-cybersecurity/		
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 bbs.antiy.cn 安天公益翻译板块		
摘要	在“随处办公”的时代，构建可扩展且与框架一致的网络安全协议尤为重要。为实现这一目标，公司可以采取 MAP 策略：管理、自动化和确定优先级。全面的 MAP 策略可以分为六步走：（1）获得全部资产的可见性；（2）实现设备管理的现代化；（3）确保设备安全；（4）确保用户安全；（5）保护边界；（6）监控并进行改进。		
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。		

成功进行网络防御的六个方法

丹尼尔·斯派塞

2022 年 5 月 4 日

Ivanti 与 Cyber Security Works 和 Cyware 合作发布的勒索软件年终报告指出，目前共有 157 个勒索软件家族，比上一年增加了 32 个。

勒索软件通常瞄准未修补的漏洞并将零日漏洞武器化，会造成严重的后果。勒索软件不断发展，它们不断寻找新的方法来破坏有价值的组织网络并扩大攻击范围，以实施和触发高影响力的攻击。

当然，随着勒索软件威胁的增加，防御策略也在不断改进。这些策略能够为企业提供保护，显著减少此类攻击产生的破坏性影响。

网络安全之旅 MAP

防御策略旨在减少攻击面和主动扫描/监控威胁，从而减少用于防御的时间和人力资源。

在“随处办公”的时代，构建可扩展且与框架一致的网络安全协议尤为重要。为实现这一目标，公司可以采取 MAP 策略：管理、自动化和确定优先级。

第一阶段“管理”侧重建立企业的网络安全基础。第二阶段“自动化”旨在减轻 IT 团队的负担。第三阶段“确定优先级”描绘了 IT 如何识别并针对最高风险领域采取行动。

全面的 MAP 策略可以分为六步走：

第 1 步：获得全部资产的可见性

企业无法管理看不到的东西。涵盖所有连接设备和软件，并可以增强资产可见性的自动化平台，有助于提供“所有资产都是如何被使用的”情境信息。这些信息对企业的 IT 和安全团队至关重要，有助于他们制定精细、有效的决策。

通过全面部署该措施，企业可以识别从公司拥有设备到自带设备 (BYOD) 的所有资产。这样一来，企业就可以了解“谁”在使用、如何使用以及何时使用这些设备，更重要的是，使用这些设备访问什么内容。安全团队可以利用这些信息来改善资产保护措施。

第 2 步：实现设备管理的现代化

在远程和混合办公环境中，提高安全性的一个重要措施是实现设备管理的现代化。为了在保护企业数据安全的同时最大限度地保护用户隐私，企业应实施完全支持 BYOD 的统一端点管理（UEM）方法。

UEM 架构通常包括通过基于风险的补丁管理和移动威胁防护来保护设备的能力。它还可以轻松监控设备状态并确保合规性，并快速、远程识别和修复问题。企业应选择具有管理功能的 UEM 解决方案，该解决方案可以跨越各种操作系统，并且可以在本地和通过“软件即服务”（SaaS）使用。

第 3 步：确保设备安全

良好的设备安全措施不仅仅在于补丁管理，还涉及部署多层次、主动的方法。企业应确保，能够访问业务资源的设备都符合安全要求，这有助于减少数字攻击面。

企业需要警惕和识别各种设备漏洞（易受攻击的操作系统版本、越狱设备等）、应用程序漏洞（可疑的应用程序行为、安全风险评估等）和网络漏洞（不安全的 Wi-Fi、恶意热点等）。实现日常安全任务的自动化，可以帮助企业实现良好的设备安全。

第 4 步：确保用户安全

一旦攻击者获取了用户的口令，就会利用这些口令执行攻击。在数据泄露事件中，登录凭证仍然是最受欢迎的数据类型——61%的事件涉及凭证窃取。单点登录（SSO）解决方案尤其容易遭受攻击，这是因为 SSO 会导致单点故障，黑客可以利用该故障来访问大多数甚至所有企业应用程序。

那么，企业该怎么办呢？他们可以通过零登录进行无口令身份验证。例如，企业可以使用多因子身份验证代替口令，这样可以提供更安全的防御层。这些多因子身份验证的例子包括：本身拥有的内容、情景信息或固有特征（生物特征，如指纹和人脸等）。

第 5 步：保护边界

随着“随处办公”的兴起，能够满足办公室需求的网络边界已经不够高效了。因此，企业必须根据“软件定义边界”（SDP）的原则建立其网路。SDP 可以集成到现有的安全系统中，以利用经过验证的标准组件。值得注意的是，SDP 也需要额外的安全层才能获得最大

收益，这个额外的安全层就是“零信任网络访问”（ZTNA）。

第 6 步：监控并进行改进

在评估安全态势方面，企业存在一个重大的问题：他们通常是在攻击发生后才做出反应。此外，企业还缺乏 IT 人才。两相结合，会导致严重的问题。为了减轻威胁并保持合规性，进行“监管、风险和合规性”（GRC）管理势在必行。企业 IT 团队需要寻找一种解决方案，快速轻松地导入监管文档，以将引文与安全和合规控制措施关联起来。此外，企业应采用自动化手段执行重复性的监管任务，将 IT 团队解放出来，以监控网络安全防御方法。

结论

借助正确的综合、集成解决方案，企业可以减轻 IT 团队的负担，保持有效、高效和直观的用户体验。这样一来，无论员工选择在何处、何时或如何办公，企业都可以保持资产的完整性和安全性。

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，同时在多地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*