简译版

如何实现更好的网络安全保障

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	How to achieve better cybersecurity assurances and improve cyber hygiene		
原文作者	菲尔·刘易斯（Phil Lewis）	**原文发布日期**	2022 年 4 月 11 日
作者简介	菲尔·刘易斯是 Titania 公司的首席执行官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/04/11/reduce-cyber-attack-risk/		
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	本文所述三个措施可以帮助企业实现更好的网络安全保障，改善网络安全：（1）进行网络分段，将企业网络拆分为多个子网络；（2）满足合规性要求；（3）采用零信任策略。		
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。		

如何实现更好的网络安全保障

菲尔·刘易斯

2022 年 4 月 11 日

企业应如何降低网络攻击成功的风险并创建可防御的网络呢？

不要做以下三件事：

不要想当然地认为，网络工程师在进行网络更改以满足运营要求时不会错误配置设备（包括防火墙、交换机和路由器）。

人为错误会造成非常严重的安全风险，这通常不是出于恶意意图——只是因为疏忽。技术人员可能会无意中错误配置设备，导致它们不符合网络策略，从而造成漏洞。如果企业没有对设备进行密切监控，那么这类配置错误可能会导致重大的业务风险。

不要低估未分段网络带来的风险。尽管它们可以提高运营效率并降低网络复杂性，但是带来的风险远大于回报。

实际上，在多起攻击事件中，如果受害企业妥善地进行了网络分段，则攻击造成的破坏会小很多。我们以 2017 年信用巨头 Equifax 的数据泄露事件为例，攻击事件发生后，Equifax 与联邦贸易委员会和消费者金融保护局达成协议，最终支付了高达 4.25 亿美元来弥补受影响的人士。

不要认为，每年只对个别设备修复软件漏洞和审计边界，就能保证企业的网络安全。

企业无法像修复软件漏洞那样修复配置错误。即使进行软件补丁升级，配置错误也会持续存在，直到网络工程师发现并纠正这些错误。因此，企业需要在日常网络安全流程中不断检测和修复配置错误，这是零信任安全策略的第一步。

要想做到上述三点，企业需要改变其思维方式。企业要认识到，他们面临的安全风险非常严重，必须进行充分的安全投资，以便在它们引发严重的业务问题之前予以妥善应对。

那么，企业应该从哪里入手呢？下述三个措施可以帮助企业实现更好的网络安全保障，改善网络安全。

1. 进行网络分段，将企业网络拆分为多个子网络。一种方法是在网络中创建单独的区

域，这些区域由配置为“拒绝未经授权的流量”的安全防火墙和路由器保护。通过防止网络内的横向移动，企业可以限制攻击造成的损害。

网络分段是一种强大的安全措施，但是尚未网络安全团队充分利用。在当前攻击日益复杂的威胁环境中，企业无法保证能够成功防御网络攻击。但是，如果正确实施网络分段策略，则可以通过有效隔离攻击最大程度地减少损害。

通过精心规划的分段网络，安全团队可以更轻松地监控网络、快速识别和隔离威胁。此外，通过网络分段，企业可以更轻松、更频繁地评估各网络设备（防火墙、交换机和路由器）的关键配置错误。这有助于降低威胁的“平均检测时间”（MTTD）和“平均修复时间”（MTTR），而这两者都是安全团队的重要目标。

2. 满足合规性要求。合规性是企业管理风险的一种方式，但它往往是一个资源密集型过程，不会显著改善安全状况。这是因为，在过去，企业只需要证明设备样本是合规的就可以了，但是现在这种方法行不通了。监管机构要求企业对其网络进行持续评估。

对网络进行分段可以更轻松地管理合规性要求，并使用针对性的方法来应用合规策略。企业可以根据“敏感度”对数据进行分段，将受监管的数据与其他系统分开。例如，PCI-DSS 仅适用于持卡人数据环境（CDE），因此有效的网络分段可减少企业的 PCI DSS 合规负担。

如果企业处于联邦供应链中，则需要遵守 CMMC 或 NIST 800-171 标准。细分的网络可以帮助企业满足合规要求，使企业继续有资格从事政府合同工作。

3. 采用零信任策略。企业不能想当然地认为其网络、应用程序或员工是安全的，而是应假设已经或将要遭到攻击。采用零信任策略意味着，企业投资于员工、流程和最佳的安全自动化技术，以不断验证员工、网络和应用程序是否安全，以及业务运营、客户和数据是否安全。

越来越多的企业开始采用零信任策略。举例来说，国防部去年发布了第一个零信任参考框架，阐述了各机构为实现有效的零信任架构需要采取哪些措施。但是，要想让其他行业的企业迅速采用零信任策略以保护其网络，可能还有很长的路要走。

在上述三种策略中，最佳方法是采用零信任策略，持续评估和监控设备。这意味着企业需要检查所有内容，这是因为今天安全的设备明天可能就不安全了。无论是导致配置错误的简单内部错误，还是通过网络横向移动引发的恶意攻击，如果不反复检查和修复，企业就无

法向自己或监管机构保证网络的安全性。

传统上，评估网络的安全状态涉及对设备进行渗透测试。即使在最好的情况下，这也不够高效：很耗时，需要大量熟练的员工，而且只能测试少数设备。因此，这类评估的范围不大，节奏不频繁，会导致风险在很长一段时间内不被发现。

企业需要一种能够提供准确、及时且可操作的风险信息的工具。该工具可以帮助安全团队识别哪些漏洞会构成严重的安全风险，并及时修复这些漏洞。实现整个评估过程的自动化只是一个开始。

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*