2021年五大关键网络安全趋势

简译版

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	5 Key Cybersecurity Trends to Know For 2021		
原文作者	诺曼·刘易斯（Norman Lewis）	**原文发布日期**	2021年8月24日
作者简介	诺曼·刘易斯是一位经验丰富的数据科学家，在大数据和机器学习行业拥有丰富的工作经验。		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/network-security/5-key-cybersecurity-trends-know-2021		
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2021年，网络安全的基础是可扩展性、用户意识和多功能性。企业的网络安全策略必须跟上不断变化的网络和安全需求。只有这样，企业才能保护其网络和数据免受攻击者的侵害。首先，企业的安全策略要跟上本文所述的五项网络安全趋势。		
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。		

2021 年五大关键网络安全趋势

诺曼·刘易斯

2021 年 8 月 24 日

新冠疫情促使很多企业开始采用远程和灵活的工作方式。因此，他们必须寻找新的、更有效的方法，来应对迅速变化的后疫情数字空间。现在，全世界有数以百万计的联网办公室，其中大部分都不像传统办公室那样受到数字保护。企业办公室中的安全防火墙、访问管理系统和安全路由器等，可能无法覆盖所有远程办公人员。这会导致企业的设备和网络易受攻击。为应对这种新挑战，企业需要了解 2021 年五大关键网络安全趋势。

1) 网络攻击面大幅增加，使得数据安全自动化成为必要。

毋庸置疑，在过去的十年中，企业的网络攻击面大幅增加。即使在疫情爆发之前，企业的大部分业务交易就是通过互联网进行的；而疫情期间此类交易又迅速增加。第四次工业革命已经到来，其主要特点是“人”和机器的日益啮合。显然，在破坏网络防御方面，黑客拥有很大的发挥空间。

在 2021 年，企业应如何保护这种巨大且持续扩展的攻击面呢？首先，企业需要采用自动化的网络安全工具。他们应部署自动化扫描技术，以进行数据访问管理，并投资于事件告警工具。最重要的是，他们应开发和利用自修复软件，来应对攻击者造成的任何损害。其次，企业需要利用机器学习和人工智能技术来应对可能的网络威胁。

2) 更多地采用多因子身份鉴别（MFA）

随着远程和灵活办公的激增，将口令作为防御网络攻击的唯一保护措施已经不够了。企业必须投资于多个数据保护层。在这方面，MFA 大有用武之地。在 MFA 模式下，员工必须先通过多个设备验证其身份，然后才能访问敏感的公司数据。举例来说，远程办公的员工想要从个人计算机登录员工门户或公司的文件共享服务。在员工输入用户名和口令后，公司的 MFA 算法会向员工的手机发送一条验证短信。该短信包含用户必须输入的一次性口令（OTP）；如果员工不能输入该口令，就无法登录系统。在这种情况下，员工的手机号码必须记录在案，未经 IT 部门批准不得更改。有些公司要求员工在他们的智能手机上安装身份验证应用程序，而有些公司则使用语音 MFA。

在很大程度上，MFA 比口令更可靠。但是，由于短信和语音 MFA 不是端到端加密的，因此仍然容易受到攻击。未来，公司可以采用应用程序身份验证器，例如 Google Authenticator、Microsoft Authenticator 和 OneSpan Authenticator 等。

3) 网络安全技术堆栈

即使企业能够保护其业务数据免受外部威胁，也应为其网站和相关工作流程量身定制有效的工具和平台。该方法适用于任何领域，比如自由医学作家网站。企业必须拥有适当的软件工具（技术堆栈），以保持强大的安全态势。可靠的技术堆栈应包括基本保护工具，如反病毒软件和防火墙，以及诸如 DNS 过滤器等高级工具。网络安全技术堆栈应提供实现数据安全计划所需的框架。该堆栈应保护企业的的操作系统、Web 服务器、数据库、数字资产和自定义 Web 应用程序等，帮助企业更有效地运行应用程序和网站。因此，企业应构建先进的网络安全技术堆栈。

那么，企业应如何构建正确的技术堆栈呢？方法就是，根据企业的风险状况进行构建。举例来说，如果企业打算在 2021 年搭建网站或应用程序，则在选择网络安全技术堆栈时需要考虑以下几点。

- 应用程序中的漏洞，这取决于后端代码。不同的运行环境有不同的漏洞。
- 在线流量和可扩展性需求/可能性。企业应考虑，将来是否需要向平台添加数据，功能性和一致性是否是其长期架构策略的一部分？如果是，则企业的网络安全技术堆栈应该是可扩展的。
- 成本，包括前期成本和长期成本。
- 使用可提供隐私、匿名性和保护的住宅代理。
- 是否有来自信誉良好的第三方库的构建块。某些堆栈带有第三方供应商库，这些库会扩展企业的网络攻击面。
- 内部 IT 团队的技能和经验。企业要想投资于某项安全协议，应首先了解该协议。
- 安全堆栈有多复杂。如果实现堆栈花费的时间超出企业的承受能力，则不值得。

4) 移动软件安全

随着远程办公的增加，企业需要确保移动软件的安全。如今，企业员工使用他们的手机、平板电脑和 PC 等访问敏感数据。有些员工甚至通过不安全的公共 Wi-Fi 来访问这些数据。在大多数情况下，这些设备通过物联网技术连接到其他远程对象。攻击者可以监控加密的消息传递应用程序，或对不安全的移动设备执行分布式拒绝服务（DDoS）攻击。企业有责任为员工的个人设备添加额外的移动软件安全层。

5) 网络安全意识培训

许多互联网用户尚不了解常见的网络攻击方法。许多用户很容易成为网络钓鱼电子邮件等基本攻击方法的猎物。这种无知助长了网络安全案件的激增。企业应使用讲解视频对其员工进行培训，帮助他们识别和阻止各种网络钓鱼攻击和恶意软件感染。

结论

在 2021 年，网络安全的基础是可扩展性、用户意识和多功能性。企业的网络安全策略必须跟上不断变化的网络和安全需求。只有这样，企业才能保护其网络和数据免受攻击者的侵害。首先，企业的安全策略要跟上本文所述的五项网络安全趋势。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

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