聚知刊出版社
JZK publishing

网络安全趋势：展望未来（吉姆·勃姆）

王思汗

国防科技大学，安徽合肥，210012

摘要：网络安全向来备受人们关注，对于网络安全基本趋势的把控与分析在技术发展日新月异的今天显得尤为重要。本篇文章聚焦网络安全的基本发展趋势，分析出当今网络安全发展机遇与挑战并存的特点，并在此基础上讨论了当前态势下应当如何做到防患于未然。

关键词：网络安全、趋势、数据、数字化

DOI:10.69979/3029-2735.24.3.067

麦肯锡探究了三个最新的网络安全趋势，以及这些趋势对正在面临新兴网络威胁和危险的组织所带来的影响。

网络安全向来是一条永无终点的赛道，而其变化的速度正在加快。企业为了运营正不断追加投资。现在，他们正将更多的系统分层处理并融入到网络之中以支持远程办公。这不仅优化了用户的体验，还可以产生更多的价值。但所有这些也创造出了潜在的新的漏洞。

与此同时，我们的对手也不再只是单枪匹马作战了——其中包含高度复杂化的组织。这些组织可以利用集成化工具，并且具备人工智能和机器学习的能力。这种威胁的范围正在扩大，并且没有组织能够独善其身。小、中企业，各城市以及国家和联邦政府与大型企业一同面临着这些危险。即便是如今最为复杂的网络控制系统，无论其多么有效，终将难逃迅速被淘汰的命运。

在这个环境下，领导阶层必须回答一些关键的问题："我们做好了在往后三至五年的时间里应对加速数字化的准备了吗？"倘若说的更加具体些，"我们真的对理解当今的科技投资对未来产生影响的方式抱有足够的期待吗？"

麦肯锡的工作帮助了全球各个组织加固了其网络防御系统，这表明许多公司认识到在网络安全能力的方面向前迈出一步，以确保其技术保持弹性的必要性。解决方案就是通过面向未来从而加固他们的防御系统——对未来可能会出现的威胁进行预测，以及理解公司现在使用的安全防御措施和未来计划使用的其他防御措施。（见边栏，"时刻保持警惕"）

1. 三个具有大范围影响的网络安全趋势

公司只有采取更加积极且面向未来的立场，才可以处理、减轻未来的破坏。在接下里的三至五年内，我们可以预见三个主要的网络安全趋势。这些趋势横跨多项技术领域，将对各个组织产生最大的影响。

1.1 对于无处不在的数据和信息平台的需求正在增加

移动平台、远程办公和其他的改变愈加依托于对无处不在的庞大数据集的高速访问，这增加了发生泄露的可能性。2026 年，虚拟主机服务的有望产生 1831.8 亿美元的市场额。各个组织收集了更多有关客户的数据——从金融交易到电力消费到社会媒体观点的各个方面的数据——以便理解、影响客户的行为并更有效地预测需求。2020 年，全球平均每人每秒创造了 1.7 兆字节的数据。随着云端重要性的增加，企业则需要越来越肩负起储存、管理、保护这些数据以及应对爆炸性数据挑战的责任。想要进行这样的商业模式，公司就需要新的技术平台，包括可以汇集信息的数据湖泊，例如遍布环境之中供应商和伙伴的渠道资产。企业不只是在汇集数据，而是把数据进行集中化，并把他们储藏在云端，给予个人以及组织（包括例如供应商的第三方）访问的权限。

近期许多引人关注的攻击充分利用了扩展的数据

存取权限。在 2020 年的 sunburst 黑客袭击中，恶意代码在常规软件更新期间流入客户处。与此类似的是，2020 年初期袭击者利用来自顶级连锁酒店下的第三方应用泄露的员工凭证来获取超过 500 万份客户记录。

1.2 黑客们正使用人工智能技术、机器学习以及其他技术发动愈加频繁的复杂攻击

老一套的独自进行活动的黑客不再是主要的威胁。如今网络黑客活动一个可达数十亿的企业，并且具有完备的组织层级和充足的研发费用。攻击者可以使用先进的工具，例如人工智能、机器学习和自动化技术。数十年之后，他们能够做到加速他们端对端的攻击生命周期——从数周到数天或数小时，可以通过这一技术手段来实现侦察。例如 Emotet，一款针对于银行的高级恶意软件，可以改变其攻击性质。2020 年，依托先进的人工智能和机器学习技术以增加效率，它以自动化贯穿全程的方式发送了情景化的网络钓鱼邮件。这些钓鱼邮件劫持了其他邮件，并给其他邮件带来了威胁——其中一些邮件与新冠病毒通讯有关。

其他技术及手段则制造了目前已知的攻击形式，例如更加流行的网络钓鱼和勒索软件。作为一项服务的勒索软件以及加密货币大幅减少了勒索软件发动攻击的成本，自 2019 年以来每年发动攻击的数量都能翻上一番。其它类型的侵扰通常会引发这些攻击数量的迅猛增长。举例来讲，第一波新冠疫情爆发之时，即 2020 年 2 月至 3 月，全球软件勒索攻击的数量总体上增长了 148%。而 2020 年 1 月至 2 月，情景化攻击的数量则增加了 510%。

1.3 不断扩大的监管范围以及在资源、知识、人才方面不断扩大的差距将超过网络安全

许多组织缺乏充足的网络安全人才、知识以及专业技术——并且这个缺口正在扩大。大体上看，网络危机的管理难以适应数字和分析转型的激增，并且许多公司并不确定如何识别并且管理数字风险。由于这些挑战的叠加出现，监管部门正在增加对公司网络安全能力方面的指导，并同样对金融服务中的信用和流动性风险以及关键基础设施中的操作性和物理性风险给予监督与关注。

与此同时，企业面临着愈加严格的遵从要求——这是基于不断增长的个人隐私关切和引人关注的违规问题的结果。如今，大约有 100 项针对跨境数据流的管理条例。网络安全团队正在管理额外的数据并报告要求。这源于白宫关于提升国家网络安全的行政命令以及移动电话操作系统的出现。该系统可以询问用户想要使用来自个人应用程序的数据的方式。

2. 建立面向未来的防御能力

对于这些转变，我们可以看到组织中体现出的防御能力。组织可以发展这些防御能力来降低风险和缓解未来网络威胁带来的冲击。明确地说，这些能力并没有很好的映射到单个班次中，并且许多能力都可应用于超过一个班次。管理团队应该综合考虑所有这些能力，并聚焦于最与公司所处独特情形和背景相关的能力

2.1 对趋势一的回应：零信任能力和以安全为导向的大数据集

减轻因无处不在的数据需求而产生的网络安全风险需要具备四个能力：零信任能力、行为分析、弹性化的日志监测以及同态加密。

零信任框架（ZTA）。在工业化国家，现在大约 25% 的工人每周进行三至五天的远程办公。复合及远程办公、已经增加的云端访问以及物联网（IoT）的集聚制造了潜在的漏洞。零信任框架转变了网络防御的重点，使其从围绕着物理网络的静态布局中走出，进而转向用户、资产和资源，因此降低了分散化数据的风险。访问受到政策更为细致地强制执行：即便用户获准访问数据环境，他们也接触不到敏感数据。各个组织应当灵活采用零信任能力以应对他们实际面临的威胁和风险范围，达成他们的商业目标。他们还应考虑开启红队测试，以验证零信任能力的功效和覆盖范围。

行为分析。对于组织而言，受雇者是一个关键的薄弱点。分析式的解决方案可以监测到一些属性，例如访问请求或设备健康状况，并且建立起一道基准线以识别

异常的蓄意或无意的用户行为或设备活动。这些工具不仅可以使以风险为基础的鉴别或授权变得可能，还可以将预防性的响应措施和应急响应措施有机结合。

针对大数据集的弹性化日志监测。由于大数据和物联网技术进步而产生的巨量数据集和离散化日志使得监测活动的挑战变得复杂。弹性日志是一种基于多种开放平台的解决方案，将其加以结合使用时，各个企业将被允许从组织的任何地方获取日志数据，并放置进一个单独的区域进而加以实时化地搜索、分析数据并使数据可视化。核心工具中的本地日志抽样功能可以减轻一个组织的日志管理负担，并且可以帮助组织识别潜在的缺陷。

同态加密。这个技术允许用户在工作时使用加密数据且无需首先解密数据，因此第三方和内部的合作者可以更加安全地访问大数据集。这项技术也可以帮助企业满足更加严格的数据隐私要求。近期在计算能力和表现方面取得的突破使得同态加密技术现在更加贴近实际，其应用范围也更加广泛。

2.2 对趋势二的回应：利用自动化技术来抵御逐渐复杂的网络攻击

为了应对受人工智能和其他高级手段驱动的更加复杂的攻击，各组织应当采取一种以风险为基础的方法，从而达到自动化和自动回应攻击的目的。自动化技术应聚焦于防御能力，诸如安全运营中心（SOC）的对策和劳动密集型互动，例如身份、访问管理（IAM）和报告。人工智能及机器学习应当应用于了解正在发生变化的攻击模式的最新情况。最终，自动化技术以及组织对恶意勒索软件威胁的自动回应的发展可以减轻受到攻击时的风险。

通过以风险为基础的方法实施的自动化。由于数字化水平的加速提高，各组织可以利用自动化处理低风险和繁琐过程，进而将资源抽离出来，留给更高价值的活动。关键在于，自动化决策应当基于对风险的评估与分割，以确保不会在无意之中产生额外的漏洞。举例而言，各组织可以对低风险资产应用自动化的补丁、配置以及软件升级，而对高风险资产进行更多的直接监督。

使用防御性质的人工智能和机器学习以期实现网络安全。由于攻击者采用了人工智能和机器学习技术，网络安全团队将需要进化、升级相同的能力。具体来说，各组织可以使用这些技术和离群模式来检测并修补异常的系统。团队也可以充分利用机器学习来优化工作流和技术堆栈，使得资源逐渐能够以最有效的方式被利用。

参考文献：

[1]《财富商业洞察》
[2]《信号化的世界：从边缘到核心》，约翰·甘兹、戴维·赖因泽尔、约翰·赖宁
[3]《数据不会休息 6.0》，多莫
[4]《马里奥特揭露分支机构泄露高达 520 万人的数据信息》，大卫·乌贝蒂
[5]《网络安全：骇客成为创收达 3000 亿美元的产业》，保险信托公司
[6]《网络安全热点数据、趋势与事实》，布莱恩·卡尔逊

译者：王思汗 1999/3/19 国防科技大学 硕士研究生
籍贯：安徽合肥