

简译版

2022 年五项网络安全预测

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	Five cybersecurity predictions for 2022 and beyond		
原文作者	安德鲁·霍华德 (Andrew Howard)	原文发布日期	2021 年 12 月 23 日
作者简介	安德鲁·霍华德是 Kudelski Security 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/2021/12/23/five-cybersecurity-predictions-2022/		
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	本文对 2022 年及以后的网络安全情况做出了预测。(1)勒索软件攻击事件会翻倍, 甚至三倍; (2)纯 OT 攻击即将来临; (3)医疗生态系统将成为主要攻击目标; (4)混合办公将进一步降低企业的安全性; (5)首席信息安全官(CISO)面临新的挑战。		
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。		

2022 年五项网络安全预测

安德鲁·霍华德

2021 年 12 月 23 日

2021 年发生了一些迄今为止规模最大、影响最大的网络攻击。今年，网络安全领域的领导者面临着诸多挑战；未来几年，他们很可能会遇到更大的障碍。

在下文中，我们将对 2022 年及以后的网络安全情况进行预测。

1. 勒索软件攻击事件会翻倍，甚至三倍

企业应专注于其网络安全以及端点检测和响应策略，而非制定勒索软件备份策略。换句话说，企业不应只关注症状，而应关注根本原因。

随着勒索软件攻击的增加，越来越多的企业选择支付赎金以换回宝贵的数据。对企业来说，“是否支付赎金”是道德感和实用性之间的两难选择。在微观层面，如果企业没有为攻击做好准备，可能会进行成本效益分析来决定是否支付赎金。然而，在宏观层面，企业支付赎金会激励更多的攻击，导致勒索软件问题加速。在微观与宏观层面的激励结构达到一致之前，企业将一直处于勒索软件的恶性循环中。

2. 纯 OT 攻击即将来临

未来，越来越多的供应链将成为勒索软件攻击的受害者。攻击者还可能以托管安全提供商和律师事务所为目标，以便同时攻击他们服务的数百个客户。企业经常依赖第三方供应商来补充他们的业务；然而，许多企业没有统一的网络安全策略和实践。甚至有第三方供应商通过远程访问技术定期维护企业的多个 OT 站点，这导致运营链中存在可利用的漏洞。随着制造供应链越来越自动化并严重依赖远程访问，企业领导者必须构建以网络安全为导向的多层网络安全战略。

制造企业应实施良好的网络安全实践和流程来保护远程访问，这是保护其免受攻击的最有效方法之一。然而，很多企业认为投资网络安全的成本太高，而且会扰乱其运营并可能延迟供应链中的产品运输，因此在这方面的投资不足。这导致他们缺乏对其 IT 和 OT 网络的可见性，无法识别需要保护的远程访问点。

随着黑客的攻击手段越来越复杂，制造企业应将防御作为首要任务。他们可以通过营造网络安全文化并实施正确的策略（例如最低权限原则），来增强其网络安全态势。此外，企业建立供应链管理计划，以确保与所有承包商和第三方供应商的网络安全实践保持一致。

3. 医疗生态系统将成为主要攻击目标

新冠疫情对医疗系统带来了巨大的压力，潜在攻击者认为攻击医疗系统可以为他们带来丰厚的回报。从医院到医生办公室和血库，医疗组织遭受的攻击大幅增加。攻击不太可能针对实际的医疗系统或设备。相反，攻击者倾向于以医院计费系统、患者记录和 ERP 系统为攻击目标。

为了保护存在漏洞的 IT 系统，医疗组织应该购买和部署强大的身份管理解决方案，以支持多因子身份验证，对其网络进行分段以减少入侵后的扩展机会。此外，他们应妥善保护关键系统，及时修复其漏洞。

4. 混合办公将进一步降低企业的安全性

随着越来越多的企业采用混合办公模式，其技术安全性会提高，而员工的个人安全性会降低。在远程办公的模式下，员工/雇主关系正在演变为交易关系，并且相互之间缺乏信任。这导致员工在保护企业方面缺乏责任感，对内部安全培训计划的认可度降低。随着“Z 世代”（Gen Z）进入劳动力市场，越来越多的人认为政府应承担保护数据的主要责任，而员工对企业缺乏忠诚度会对已经存在的隐私问题产生负面影响。

5. 首席信息安全官（CISO）面临新的挑战

2022 年，CISO 应了解担任该职务所需的技能和资格。他们不仅需要监管多个领域，包括安全运营和身份管、风险管理，以及监管和合规问题，还要承担着更广泛的职责。

企业将对安全和风险管理计划进行更多投资，这意味着 CISO 会成为管理团队的一员，更频繁地向其他领导报告进展情况。董事会开始着手了解安全问题，而许多企业仍存在老旧的问题，因此首席财务官（CFO）可能很快就会要求安全投资获得回报。CISO 需要衡量当前的成熟度，以确定其目标，并设计一种方法来计算策略、计划和活动如何满足董事会的要求。随着高管和董事会对网络安全问题的关注，CISO 将承担更大的责任和压力，以保护企业免受不断涌现的新威胁。

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>