2021 年的网络安全重点

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	2020 set the stage for cybersecurity priorities in 2021		
原文作者	奇·威特（Chip Witt）	**原文发布日期**	2020 年 12 月 31 日
作者简介	奇·威特是 SpyCloud 产品管理副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2020/12/31/2021-cybersecurity-priorities/		
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		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公有方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

2021 年的网络安全重点

奇·威特

2020 年 12 月 31 日

新年即将来临。2020 年是压力满满的一年，新冠疫情、政治斗争和社会动荡等问题层出不穷。

对于网络犯罪分子和诈骗者来说，2020 年则是非常活跃的一年。他们利用人们的恐惧心理和漏洞来实施新的骗局。例如，他们伪造政府健康网站，诱骗人们点击包含恶意软件的链接；他们针对送餐应用执行撞库攻击；他们冒充“美国疾病控制和预防中心”（CDC）发送网络钓鱼电子邮件等。

不幸的是，在 2021 年，疫情仍会持续下去，网络犯罪活动也会如影随形。在新年即将来临之际，我们来回顾一下 2020 年的攻击趋势，并对 2021 年的网络安全趋势进行预测。

1. 工作和个人账户的混淆导致漏洞增加

2020 年初疫情爆发时，企业停业，学校停课，数百万父母和孩子不得不在家办公和学习。这种现象导致孩子们使用父母的设备、账户和凭证进行在线学习和娱乐。

65%的成年人承认，他们跨多个账户重复使用口令。在家庭成员之间，这一做法更加普遍。美国国家标准与技术研究院（NIST）对美国两所学校三至八年级学生进行的一项研究发现，孩子们对口令安全的理解是不错，但是他们仍然倾向于对所有账户使用相同的口令(三-五年级的比例为 58%，六-八年级的比例为 78%）。在父母返回办公室办公，孩子回到学校上课后，即使只有一个应用或一个软件发生数据泄露，也可能会暴露其他家庭成员的多个账户。

2. 企业级网络保护扩展到个人账户

当攻击者发现高价值目标时，他们会寻找任何易攻击的入口点。正如窃贼检查每扇门和窗户是否未上锁一样，寻求业务数据的网络犯罪分子可能会通过某人的个人电子邮件账户发现薄弱环节。跨工作和个人账户的口令重用，以及个人设备上的凭证窃取恶意软件，会为攻击者窃取公司数据打开大门。

安全团队正在努力应对这样一个事实：针对特权用户的攻击规模和破坏程度不断增加，对许多企业来说，这些用户的个人账户是巨大的负担和安全盲点。但是，犯罪分子的目标不仅仅是高管，HR 员工、工资单、财务、开发人员和系统管理员都有可能是他们获取有价值信息的途径。我预测，到 2021 年，随着企业对威胁的了解日益加深，更多的安全团队会将企业级监控和保护扩展到有价值的、易受攻击的个人账户。

3. 零售商首当其冲遭遇网络诈骗

全球疫情导致网络零售活动蓬勃发展。在压力山大的 2020 年，消费者使用电脑从各个网站购买必需品和医疗用品，这些网站既包括亚马逊等大型网站，也包括诸多小型电子商务网站。诈骗者利用这一趋势执行了一系列诈骗活动，最终侵害到了零售商的利益。

对于零售商来说，这个假期已经很艰难了——由于经济原因，消费者的出行减少了，花费也减少了。而诈骗者劫持账户、冒充买家和拦截货物，进一步加剧了零售商的困境。零售商希望使购买过程快速简便，以减少与顾客的摩擦，但这也使犯罪分子更容易执行攻击。恐怕在 2021 年初，大量“拒付”将使假期中零售商的利润大打折扣。

4. 勒索软件继续猖獗

2020 年上半年，11 起最严重的勒索软件攻击给各市、大学和企业造成了高达 1.44 亿美元的损失，每起攻击的平均损失超过 1300 万美元。由此可见，这是一种非常有利可图的攻击模式，因此犯罪分子不会放弃此类攻击。

即便美国财政部声称要惩罚支付赎金的公司，公司还是倾向于支付赎金，因为这是恢复业务的最快方法。即使攻击者索要的赎金不断增加，公司仍然选择支付赎金，这进一步激励了攻击者。

疫情对此也有影响。各种类型的组织转向远程办公和远程学习，使得他们更容易遭受网络攻击。越来越多的医院和医疗公司成为攻击目标，因为诈骗者知道他们宁愿支付赎金，也不愿冒可能造成更大损失的停机风险。

5. 从疫情相关的诈骗中恢复

我们预计，在许多方面，2021 年将成为复苏的一年。我们有望摆脱疫情，但是经济或其他方面的复苏可能还需要一段时间。

正如上文所述，在 2020 年，网络犯罪分子非常忙碌，他们利用人们对疫情的恐惧心理，窃取信息并利用窃取的信息劫持账户，以执行各种形式的诈骗活动。据 SpyCloud 统计，今年，每月有超过 10 亿个凭证被盗。攻击者通过诈骗网站、恶意软件和数据泄露等窃取了这些凭证。这会产生长期的影响——在 2021 年，账户劫持的受害者需付出大量时间来应付这些影响。

企业需要采取措施保护自己和个人用户。越来越多的公司将网络安全视为对客户的基本责任。对于最受信的公司来说，保护网络安全是指导原则之一。当考虑新年目标时，每个人都应该将网络安全列入目标清单。在我们恐惧新冠病毒的同时，犯罪分子也在试图利用我们的恐惧心理。

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