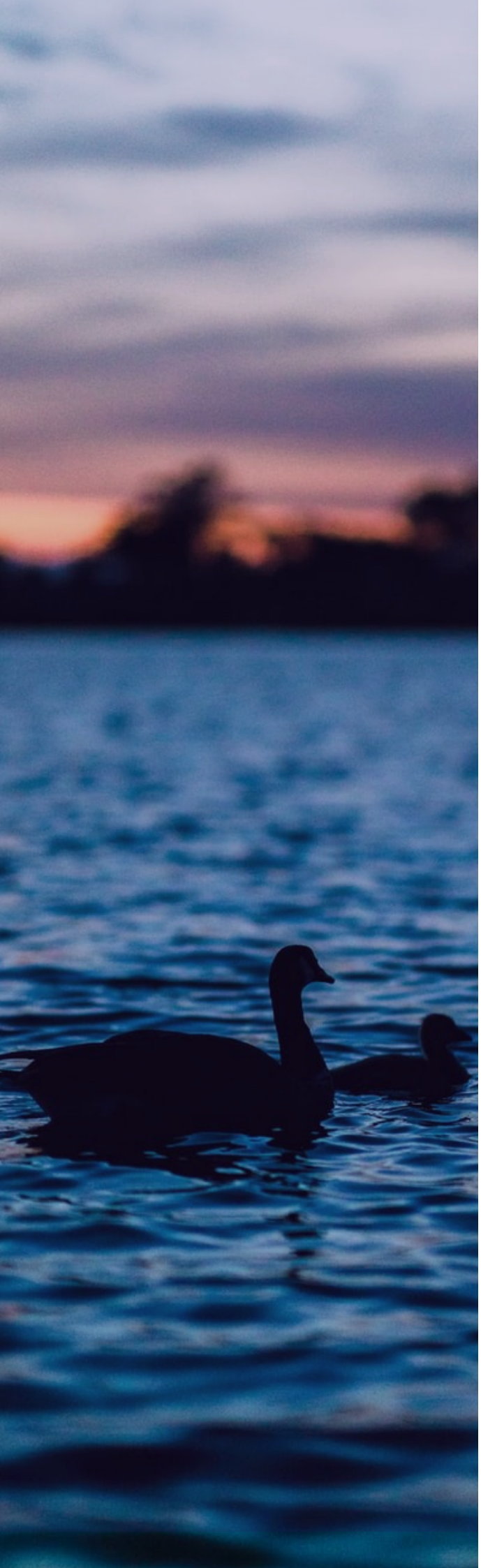
后疫情时期
初创企业安全生存指南

知道创宇

本指南旨在为创业公司提供一个低门槛、低成本并且高效的安全建设指南，让创业公司可以有更多的精力投入到业务发展上，避免安全问题造成致命打击。对创业公司来说，安全投入不必过多，但是绝不能忽视。

目录



序

2020年初，疫情黑天鹅突然降临，全球原本的发展节奏被打乱，众多创业公司更是危机重重。截至五月初，国内的疫情已得到有效控制，然而，国外的抗疫行动正面临严峻挑战。置身全球化进程的今天，国内企业如何规避后疫情时期带来的不利影响，依然是个难题。

对创业公司来说，确保充足现金流成为度过难关的首要条件。头部创业公司估值暴跌，融资受挫哀声连连；而中下游创业公司，或将面临更棘手的资金问题。

但是我们换个角度来看，“大疫之后必有大变，大变之后也会孕育新的机会”。

现在，创业公司似乎撑过了至暗时刻，所有人都在等待触底反弹。低谷时期也不能懈怠，需要调整心态，打磨产品，做好迎接一切机会的准备。

后疫情时期要寻求稳定甚至是增长，业务的稳定运营就必须要保证。而安全，正是其中最易忽视的关键点。安全问题发生前，存在感低；发生以后，损失难以挽回。

而事实正是：当今一切的数字化，都离不开安全。

十万中国创业公司正在等待寒冬渐去

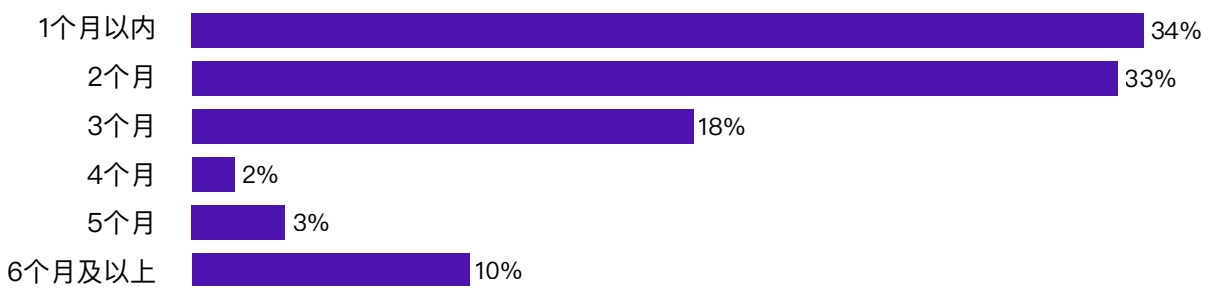
根据中欧商业评论2020年2月5日发布的《清华、北大联合调研995家中小企业》报告显示：”34%的企业账上现金只能维持1个月，33.1%的企业可以维持2个月，17.91%的企业可以维持3个月”。就是说，85.01%的企业最多能维持3个月，仅有不到10%的企业现金能维持6个月以上。

再看融资方面，据鲸准研究院发布的《2019年股权投资白皮书》显示，即使是在疫情发生前的2019年，创投市场总交易数量已经降至少于4000起，降幅达到61.9%。那些把希望寄托于融资的创业公司，现在更是雪上加霜。

收入暴跌，融资遇阻，这让许多甚至还未开始盈利的创业公司已经走到了商业的终点。

（资料来源：36kr）

现金维持时间



（数据来源：中欧商业评论）

后疫情时期，创业公司如何精益增长

这次疫情提醒我们，在未来黑天鹅可能是常态，让公司具备应对黑天鹅事件的能力，也是实现增长条件之一。

其中有两个要点，对创业公司来说格外重要。

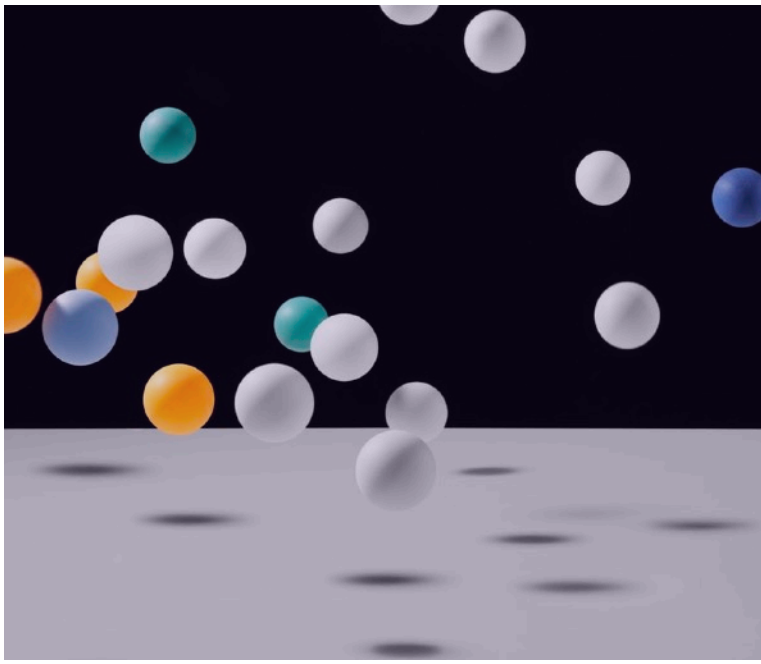
1反脆弱

风险管理理论学者纳西姆·塔勒布在他的著作《反脆弱》里提到，世间万物都可以用三元结构来概括——脆弱态、强韧态和反脆弱态。

脆弱态好比一个玻璃球，很坚硬、但是从高处摔落的时候很容易就摔碎了；强韧态像是塑料皮球，看起来柔软但是掉到地上丝毫无损、可以平稳落地；而反脆弱态就像乒乓球，落地不仅不会受到损伤还可以弹得更高。

所以脆弱态真正的反面不是强韧态，而是反脆弱态。强韧态是抵御风险的能力，而反脆弱态是能够从危机和风险中获利。

（资料来源：高榕资本）



2二八定律

意大利经济学家帕累托提出，约仅有20%的变因操纵着80%的局面。也就是说：所有变量中，最重要的仅有20%，虽然剩余的80%占了多数，控制的范围却远低于“关键的少数”。

在企业管理中，这个定律依然适用。企业20%的投入，决定了80%的营收。

以上这两点，都与安全相关。安全，帮助企业打好反脆弱态的地基；安全，是20%投入里的一笔，却影响了了80%的营收。

创业公司为什么要做安全建设？

防损

很简单，也很直接。安全问题一旦发生会给创业公司直接带来巨大损失，非业务本身方向问题导致创业公司夭折，令人惋惜。

试想，创业公司艰难克服了从种子期到早期的各种困难，产品在不断迭代与尝试下终于找到了真正的市场匹配，开始迎来高速发展的成长期，如果在这时暴露出重大安全问题，将会打乱整个发展节奏，甚至影响资本的进入。

因全球疫情原因飞速增长的视频会议软件Zoom就因安全问题爆出，引发了全网的信任危机。去年12月至今年1月初，Zoom的股价还维持于60–70美金，三月以来高点达到160美金。在一连串产品安全问题爆出之后，股价回落到120美金。

可以看出，市场的预期并不会对Zoom的优势地位进行偏袒，用户也不会因为产品好用，就放弃对安全的追求。

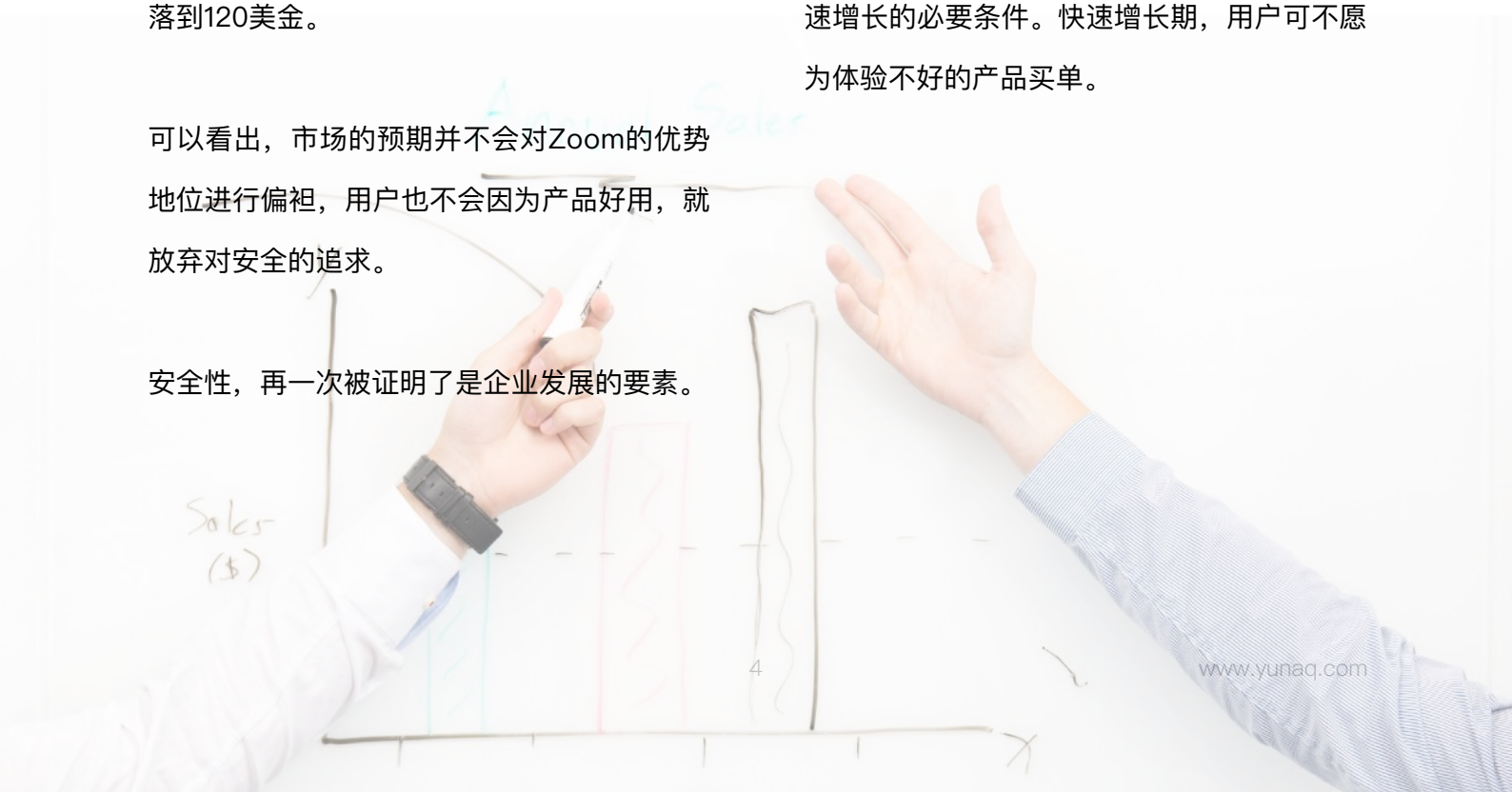
安全性，再一次被证明了是企业发展的要素。

增长

孵化了100多家创业公司的商界传奇Bill Gross曾在TED里演讲到：创业成功的重要因素之一是抓住时机。

他拿Airbnb举例，最初很多聪明的投资者都没有投资，因为大家觉得：“没有人会把自己家租给陌生人”。当然，用户证明这种想法是错的，Airbnb恰恰创立于经济周期中的“经济萧条”时，人们非常需要额外收入，这也许有助于人们对钱的渴望，超过他们不想把房子租给陌生人的想法。一个好的商业模式、一个好想法，超棒的执行力外，加上重要的时机，成功变成了自然而然的事。

而业务的稳定和安全，是创业公司抓住时机快速增长的必要条件。快速增长期，用户可不愿为体验不好的产品买单。



合规

我国在2017年6月1日起开始正式实施《中华人民共和国网络安全法》，这意味着安全意识薄弱不再成为网站被黑的理由，网络运营者需要担起网络安全的责任，创业公司也不例外。其中比较重要的几点为：

1企业应对网络运行安全负责

企业应按等保要求来保障网络运行安全，要有相应的制度与规程，要有主体负责人，要有技术防范措施，要有监管手段，并做好容灾措施。

2企业应为网络产品提供持续安全服务

企业在做网络产品研发时需先考量自身是否存在漏洞，并且要对这种安全性做持续观察，以及在用户端有持续的安全体现。

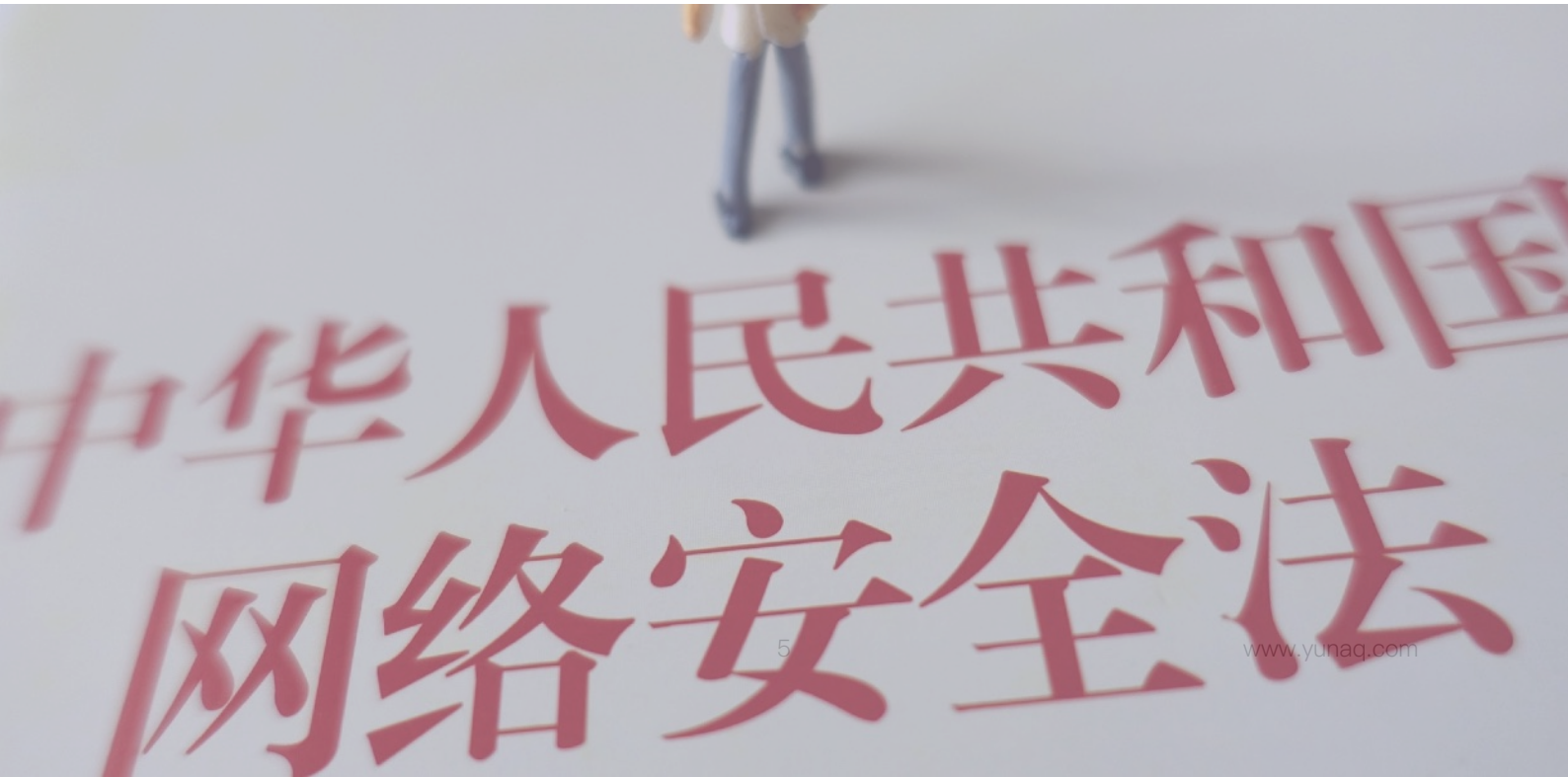
3企业网络用户需实行实名认证

实行网络用户实名认证是落实网络不是法外之地的重要措施，企业应负有这一责任，而将其作为法规写入《网络安全法》形成规定也是一种必要之举。

4企业应对用户信息做好严格保密

网站的用户个人信息泄露一直是网络欺诈犯罪治理环节上的顽疾，对于企业来讲，此处相应的法律责任也更重，这就需要为线上服务部署提供最佳的安全防护才行。

除此之外，等级保护2.0的正式实施也让各行业有了安全建设的规范标准。



不同阶段的创业公司，需要什么样的安全措施

初创

关键点：保障业务顺利上线

创业公司在早期，目标就是尽可能久地活下来。为了找到市场机会产品会快速迭代，不断探索调整业务方向，这也意味着在创业公司业务快速发展的同时，运维策略和研发过程都可能不太规范。

为了保障业务顺利上线，有这几点安全工作是必须要做的。

1 为网站、APP、小程序等业务系统安装数字证书（SSL证书）

SSL证书是数字证书的一种，它的作用是在客户端浏览器和Web服务器之间建立一条SSL安全通道。

不安装SSL证书，采用HTTP通信，就是不加密的通信。所有信息以明文的形式传播，这会带来三大风险。

- 窃听风险：第三方可以获知通信内容。
- 篡改风险：第三方可以修改通信内容。
- 冒充风险：第三方可以冒充他人参与通信。

除此之外更为重要的是，SSL证书已经是业务上线的基本要求。Chrome（谷歌浏览器）、Safari（苹果浏览器）等常见浏览器都将未安全SSL证书的网站标记为不安全，AppStore和微信小程序也明确要求未安装SSL证书的APP和小程序不得上线。

好在创业公司在SSL证书上的花费并不会太高，现在市面上许多有免费的证书可以选择。当然，如果有更高安全的需求，也可以选择付费购买。

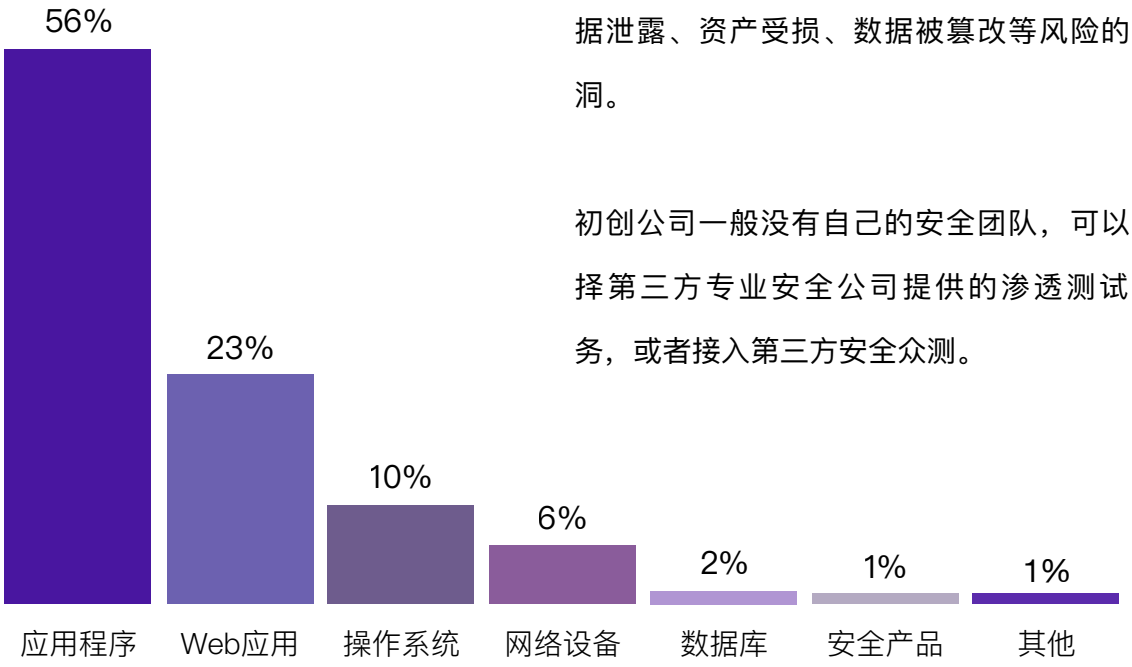
2上线前对业务系统进行安全检测

根据国家互联网应急中心发布的《2019年我国互联网网络安全态势综述》的数据显示，2019年，国家信息安全漏洞共享平台(CNVD)收录安全漏洞数量创下历史新高，共计16193个。

2019年收录的安全漏洞数量中，按影响对象分类统计，排名前三的是应用程序漏洞、Web应用漏洞、操作系统漏洞 。

从数据可以看出，不管是什么样的业务系统，大部分都会被漏洞影响。要保障业务顺利上线，安全测试必不可少。

漏洞影响对象占比



（数据来源:国家互联网应急中心《2019年我国互联网网络安全态势综述》）

初创公司可以使用免费开源的漏洞扫描工具如：OpenVAS、Nikto。但免费工具也意味着对开发者的安全素养要求较高。

如果没有专业的安全运维人员，可以使用商业的漏洞扫描工具，扫描后会出具报告以及修复建议。

漏洞扫描只能基于漏洞数据库对系统的安全脆弱性进行检测，通常是作为渗透测试的前奏。如果是正式对外上线并且有大流量的业务系统，建议在上线前需要对系统进行渗透测试。

渗透测试是模拟黑客攻击对业务系统进行安全性测试，可以比黑客更早发现导致企业数据泄露、资产受损、数据被篡改等风险的漏洞。

初创公司一般没有自己的安全团队，可以选择第三方专业安全公司提供的渗透测试服务，或者接入第三方安全众测。

3接入免费或者低费用的云安全产品

云安全产品有天生的优势，方便、易用、门槛低，而且一般产品都是按需付费，对初期的创业公司来说，是控制成本的绝佳方式。

创业公司如果已经接入了公有云厂商的云服务，可以选择云厂商提供的附带云安全产品，也可以选择专业云安全公司的产品。

为应对复杂且多变网络环境，创业公司网站通常需要接入云WAF以抵御黑客的攻击。

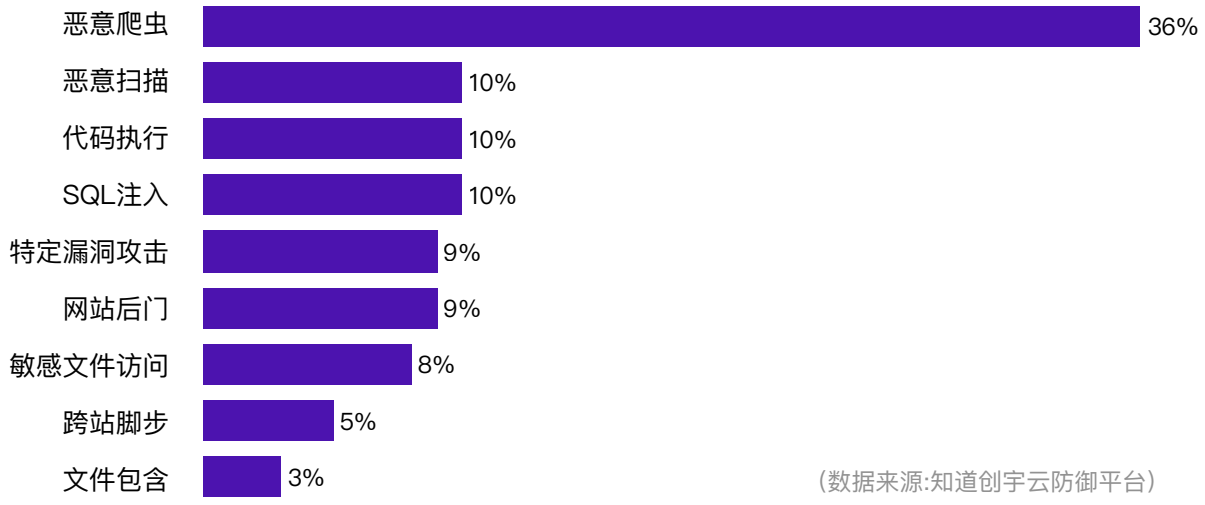
根据知道创宇云防御平台拦截的Web应用攻击数据显示，2019年攻击趋势呈现出高强度、持续性的特征。全年拦截网络攻击3321亿次，相比2018年上升12.3%。其中恶意网络爬虫攻击首次超过扫描器攻击拦截恶意爬虫超927亿次，占全年攻击总量的36%。

除此之外，网站还可以选择接入CDN，安全加速业务系统的同时减少创业公司的带宽投入。既提高用户访问速度，又减少了成本开支。

如果是高风险行业，如游戏、电商、金融等，DDoS防御也必不可少。这种流氓的攻击方式，让许多创业公司苦不堪言。由于攻击与防御成本严重倾斜，许多创业公司会面临没有资金防御攻击的尴尬境地。

因此，在前期可以通过架构布局、整合资源等方式提高网络的负载能力、分摊局部过载流量，并通过接入第三方服务拦截恶意流量。这种防御思想更为“理智”，而且对抗效果良好。

Web应用攻击类型占比



（数据来源:知道创宇云防御平台）

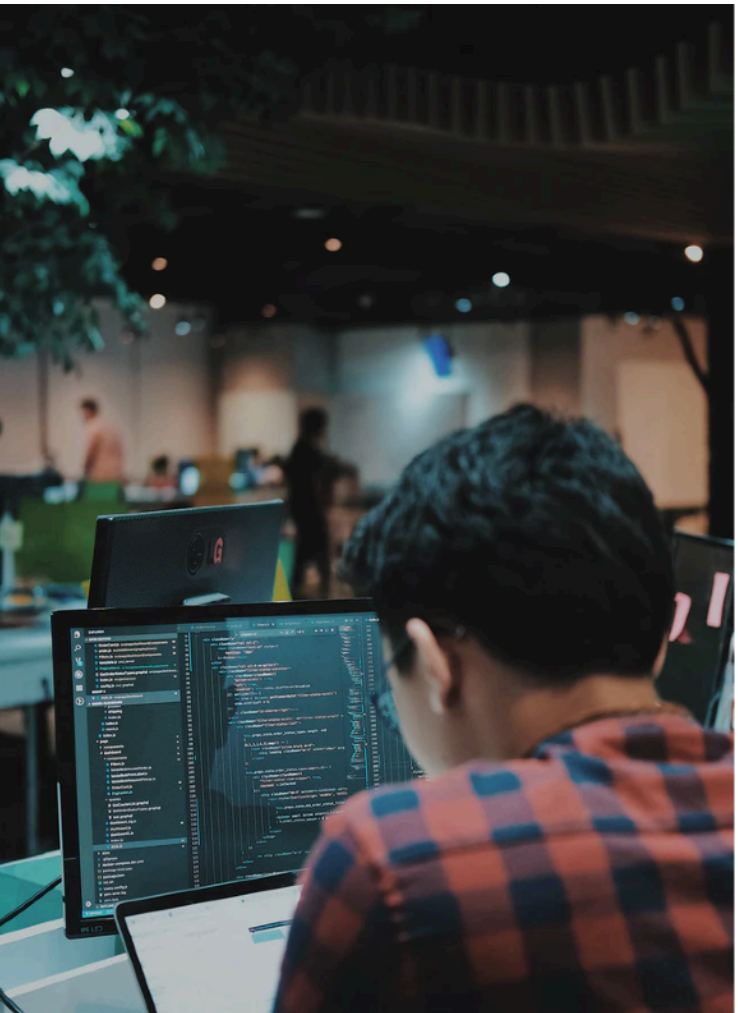
成长

关键点：让业务稳定运行

成长期的创业公司已经过跨过了初期不断迭代探索的鸿沟，开始有了较为稳定的业务模式。这个阶段是创业公司高速发展的时期，业务的稳定运行也自然成为了快速增长的保障。针对这个阶段的创业公司来说，对安全的投入需要更加用心。

1 聘请专业的安全人员

成长期的创业公司，对安全的需求更为迫切。这时，若发生安全事故，将会对快速发展的成长期创业公司带来致命打击。所以聘请专人负责公司安全，显得十分必要。



专业的事交给专业的人做，可以减少公司不必要的人力成本投入。人才是公司安全发展的根本，创业公司在成长期可以开始引入安全工程师，人数不必过多，可以隶属于公司的信息部门。

2 IPv6安全部署

随着全球IPv4地址的耗尽，以IPv6为代表的下一代互联网技术应运而生。国家层面出台《推进互联网协议第六版(IPv6)规模部署行动计划》，全力推进互联网演进升级和健康创新发展。接入IPv6已然成为业务刚需，现目前不支持IPv6等于放弃市场。

在发展的同时，IPv6的安全风险也开始显现，IPv6网络攻击数量剧增，攻击范围也在逐渐扩大。仅2019年，知道创宇云防御平台共拦截来自IPv6网络攻击9.2亿余次，总访问请求中有8.3%的请求为网络攻击。

在大量攻击的背景下，成长期的创业公司需要重视IPv6的安全部署。

（数据来源:知道创宇云防御平台）

3严格管理内部业务权限

据著名国际咨询服务公司Willis Towers Watson的网络保险理赔数据显示，2/3的网络安全问题是由于员工疏忽和渎职而直接或间接造成的。相较之下，仅有18%的网络安全问题是由外部威胁直接引发的。

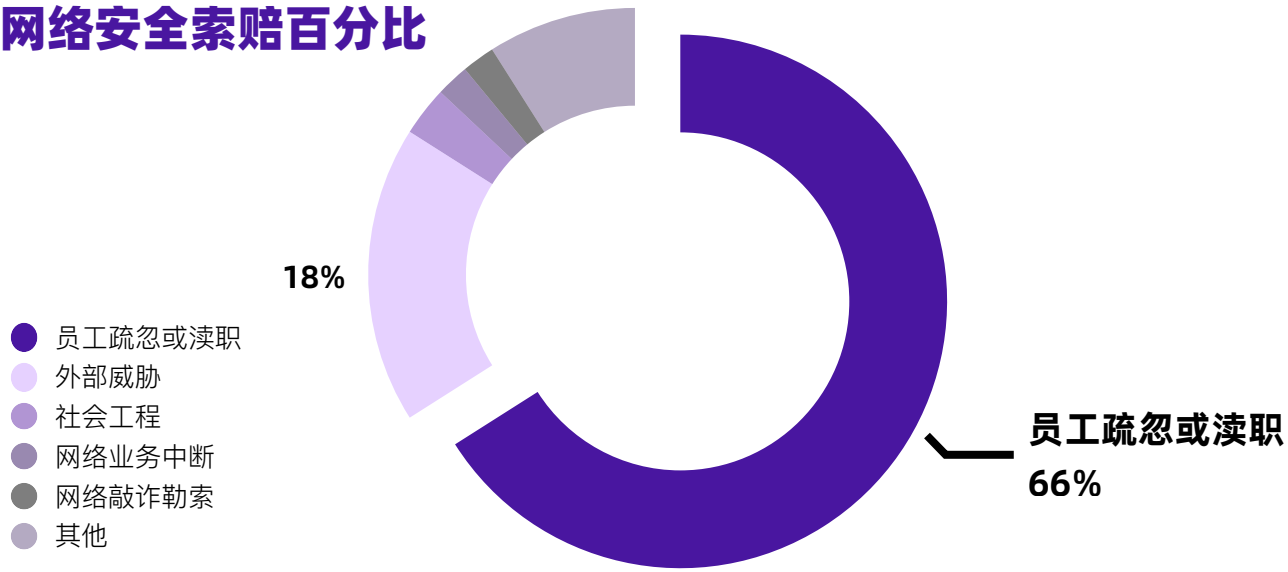
因此，成长期的创业公司必须重视内部权限管理，包括数据库、服务器、后台等各种关系公司核心资产的权限。

必要时建议开始双重验证，这样可以最大程度避免一个员工的误操作或恶意行为。

今年2月微盟数据库被删事件，直接影响了300万商家。微盟受事故影响，市值一日内蒸发超12亿港元。一场人为的破坏导致了无法估量的损失，让成千上万的商家生意停摆。

这次事件再次给业界同行敲响警钟：数据安全管理无小事。所以企业在进行数据管理需要做到两点：

- 实行严格的备份机制；
- 管理权限分开。



（数据来源:willis towers wastson）

成熟

关键点：加强安全建设

普华永道在报告《从初创到成熟，独角兽企业如何识别风险、迅速响应？》里提到：仅有39%的受访企业表示他们有危机应对计划并进行过测试，有44%的成熟独角兽企业尚没有危机应对计划及预案。

普华永道还提到：能否预测各种不确定性并适当的处理不确定性、建立有效的危机应对计划及预案，成为创业成功与否的决胜因素。

越成熟的创业公司，越依赖数字化，更应该重视安全建设。

1 打造强有力的安全团队

成熟创业公司有必要打造自己的安全团队。处于此阶段的创业公司通常也在经历B-C轮融资，或筹备上市，安全问题不应该成为资本流失的隐患。

安全团队可以帮助公司及时发现问题，他们可以全权负责公司内外部的安全建设。

2 定期进行业务安全检测

安全检测可以由自己的安全团队进行，也可以由安全公司协助完成。定期的安全检查，可以发现潜在隐患并及时修复，以确保业务系统安全性。

公司是否有一个职责明确的正式危机应对计划

（数据来源:普华永道《普华永道独角兽CEO调研2018》）

3选购贴合业务的商业安全产品

安全团队与商业安全产品的加持下，可以让安全工作更易进行。专业人员与专业工具结合，可以最大程度的提升公司安全能力。

4员工安全意识培训

前面有提到：2/3的网络安全问题是由于员工疏忽和渎职而直接或间接造成的。所以在加强权限管理的同时，成熟的创业公司需要对员工做安全培训，这时公司有能力，也有必要去做这项安全措施。

附 常见安全名词解释

云安全：

由云计算衍生而来，云安全可以一站式的提供安全与加速解决方案，以“零部署”、“零维护”、“云防御”的模式，阻止包括XSS、SQL注入、木马、0day攻击、DDoS僵尸网络、DNS攻击等一系列针对Web系统的安全威胁。

WAF：

全称Web应用防火墙，代表了一类新兴的信息安全技术，用以解决诸如防火墙一类传统设备束手无策的Web应用安全问题。

DDoS：

DDoS全称分布式拒绝服务攻击，是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。

流量清洗：

针对DDoS攻击的监控、告警和防护的一种网络安全服务。

SQL注入：

SQL注入即是指Web应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在Web应用程序中事先定义好的查询语句的结尾上添加额外的SQL语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

0day漏洞：

是已经被发现（有可能未被公开），而官方还没有相关补丁的漏洞。

中间人攻击：

指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。

弱口令：

仅包含简单数字和字母的口令，例如“123”、“abc”等，这样的口令很容易被别人破解，从而使用户的计算机面临风险。

CDN：

CDN即内容分发网络，它构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。

IPv4：

互联网协议第4版，2019年11月26日，全球所有43亿个IPv4地址已分配完毕，这意味着没有更多的IPv4地址可以分配给ISP和其他大型网络基础设施提供商。

IPv6：

互联网协议第6版，设计的用于替代IPv4的下一代IP协议，其地址数量号称可以为全世界的每一粒沙子编上一个地址IPv6的使用，不仅能解决网络地址资源数量的问题，而且也解决了多种接入设备连入互联网的障碍。

渗透测试：

模拟黑客攻击对业务系统进行安全性测试，比黑客更早发现可导致企业数据泄露、资产受损、数据被篡改等漏洞。

漏洞扫描：

基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测行为。

数字证书：

数字证书是指在互联网通讯中标志通讯各方身份信息的一个数字认证，人们可以在网上用它来识别对方的身份。具有安全性、唯一性、便利性的特点。

SSL证书：

SSL证书是数字证书的一种，类似于驾驶证、护照和营业执照的电子副本。因为配置在服务器上，也称为SSL服务器证书。如果您的网站使用 SSL 证书 (SSL Certificates)，并显示了签章 (Secured Seal)，您的客户就知道他们的交易安全可靠，并且充分信赖您的网站。

知道创宇

关于我们

知道创宇是国内最早提出云监测与云防御理念的网络安全公司之一，经过多年的积累，利用在云计算及大数据处理方面的行业先进能力，可为客户提供具备国际先进安全技术标准的可视化解决方案，提升客户网络安全监测、预警及防御能力。

对创业公司说

知道创宇可以为创业公司提供低成本的安全保护，保障创业公司在发展中不被安全问题影响或制约，用安全为创业公司发展赋能。你们来改变世界，我来守护你们安全。

关注我们

微信公众号

知乎

更多信息

了解更多知道创宇安全产品及解决方案，欢迎访问我们的官网：www.yunaq.com

也可以直接拨打安全专家热线：

400–833–1123