新冠肺炎如何改变数字资产管理

新冠肺炎如何改变数字资产管理

作者：东亚区域总监 Alban Kwan

“互联网之父”Vint Cerf 在 2019 年 9 月的一篇文章中表示：“如今，黑客们会定期破解在线账户，将用户引导至虚假网站或已攻破的网站。因此，我们需不断制定新的安全措施加以应对。如今，互联网安全创新的话题主要为**验证与确保在线人员及组织身份的安全性**[1]。”

据 Vint 称，网络身份是网络安全的一大核心问题，但网络安全圈子却鲜少提及这一话题。为什么这个重要概念并未收获更多关注呢？我认为原因之一在于网络身份的定义不够明确，这一概念超越了网络的技术因素，并牵涉到知识产权和品牌。

什么是网络身份？为了回答这个问题，我引用了一个更易于理解的术语——数字资产。数字资产指的是在与互联网上的其他人连接时，能协助建立网络形象、辨识个人身份的资产。缺少了域名、域名系统（DNS）、邮箱地址、移动应用软件或社交媒体平台等资产，企业便无法存在于网络中。数字资产属于企业的知识产权。内外部相关方需要频繁使用数字资产进行宣传，因此从网络安全和在线营销的角度来看，数字资产非常重要。

如果 Vint 言之有理，数字资产或网络身份就是企业能否取得数字成功的关键。关于数字资产管理的文章和典范做法屡见不鲜，但本文讨论的是数字资产管理在新冠肺炎疫情结束后的发展趋势。

1. 台式电脑和网络会议的兴起

Mozilla®最近开展的研究发现，台式电脑的使用率显著提升，这可能归因于全球各地实施的社交距离措施[2]。由于大部分员工只能居家办公，台式电脑成为了工作、通信和娱乐的主要工具。移动设备在出行和差旅途中更为便利，但目前人们对它们的依赖性有所降低。

至少在短期来看，手机和移动网络的使用率已经出现了下滑。据《纽约时报》的文章《改变互联网的病毒（The Virus Changed the Way We Internet）》[3]所述，主流娱乐和社交媒体品牌发现，与移动应用软件相比，桌面版网站的使用率增长幅度更大。

品牌	网站日平均流量增长	移动应用软件日平均流量增长
Facebook®	27%	1.1%
Netflix	16%	0.3%
YouTube™	15%	-4.5%

长期来看，我们预计网络会议将成为开展业务的常见方式。许多企业已经意识到，不是所有会议都需要将人员集聚在一个实体空间内——通过居家限制期间举行的一系列虚拟会议，我们发现虽然实体会议减少，但面对面互动仍不可或缺，即便是通过视频通话进行。另外，许多企业已经为移动工作环境投入良多。由于全球经济可能会面临衰退期，网络会议可以帮助组织更好地控制成本。

这对数字资产管理造成两个关键影响：

首先，无论使用台式还是移动设备，互联网运用正方兴未艾。对企业而言，建立有关品牌在互联网上存在及接触用户的渠道的基本架构（即数字资产）将变得越发重要。

随着智能手机与设备的普及，企业对数字资产的理解出现了诸多误解。其中一项误解是，由于移动互联网逐步成为主流趋势，移动应用软件才是王道，其他一切都不重要——“在浏览器里输入域名”是网址时代遗留的陋习，网站及其相关域名资产现在都可以弃之不顾了。这错得太离谱了。无论是通过移动还是台式设备进行访问，互联网都会使用 IP 地址、域名和 DNS 将企业与顾客相连。退一步说，大部分移动应用都会使用域名和 DNS，现在还有用 HTML5 开发移动应用软件的趋势，而这也是一种网站编程语言。

除了台式电脑应用增长的趋势外，移动应用软件开发还高度依赖数字资产，这进一步提醒企业不要忽视网络财产，域名和 DNS 等数字资产依然是品牌在互联网上长期存在的关键要素。

其次，我们越是依赖互联网，就越应该竭力确保互联网安全。在线会议的盛行为网络攻击打开了全新的渠道，也使网络安全变得更为复杂。Microsoft Teams 和 Zoom 开始在全球各地逐步流行，而后者则承受着名为“Zoom 轰炸”的攻击。Zoom 轰炸指的是素不相识的陌生人侵入视频会议。部分企业可能会限制添加企业外的联系人，但最终，在线会议可能会成为电话通讯、电子邮件或聊天的补充。中国大陆的状况正是如此。在中国大陆，微信、叮叮或飞书成为了企业进行业务沟通的理想选择，甚至替代了传统的电子邮箱。由于这些工具太过流行，中国大陆的参会者已经不再交换名片，而是在微信上添加好友。顾客对即时互动服务的需求很可能延续下去，向在线会议发展的趋势似乎已成定局。

在线会议和即时通讯工具也带来了安全风险，因为这些工具通常是为开放的社交沟通而设计的，也鲜有可验证对方身份的工具或方法。例如，假设某位用户通过不当手段获得了会议链接和密码，他便可以假冒真实联系人加入电话会议。这与电子邮箱不同。邮箱地址的域名便可用作身份验证，@后的域名便是真正的公司名称，还有基于域的邮件验证、报告和一致性（DMARC）和发件人策略框架（SPF）等预防欺诈的协议。然而，微信、Teams 和 Zoom 的身份识别无法对另一端的用户身份验证提供足够的保障。以我个人为例，在我的微信联系人名单中，许多人都更换了公司，也有许多人手机失窃。我也曾经收到过未知联系人的聊天邀请，他们通过我的手机号码添加了我，误以为我是手机号码的前任主人。

在这些平台上，骗子很容易使用假冒或相似的身份来欺骗员工，并成功获邀加入商务对话，窃取敏感数据或访问权限。骗子还可能伪装成企业代表，钓鱼并诈骗你的客户。

中国大陆的商务通讯工具上存在着许多类型的钓鱼诈骗和社交工程骗局[4]，许多恶意人士在寻找能够滥用谋利的任何漏洞，包括 Teams 和 Zoom。和企业邮箱一样，微信或 Zoom 的身份验证也是企业需要积极管理的数据资产组合。无论这一趋势今后如何发展，这都体现出了数字资产管理核心原则的重要性——你必须对自己拥有的资产和身份识别信息进行妥善考量与管理，才能辨别真伪。

2. DNS 滥用

我曾经在一篇文章中探讨过业务连续性方案实施过程中的安全盲点，并谈论了新冠肺炎期间的虚拟专用网络（VPN）和 DNS 劫持风险。在后新冠时代中，这种风险很可能继续存在，也可能转变为其他形式。

许多企业可能已经习惯了远程工作安排，架设了 VPN 或制定了远程工作政策。这意味着企业可能会继续远程办公，或者采用其他弹性工作安排。然而，并非所有企业都考虑到了远程办公环境的其他网络安全风险，他们的基础设施依然是为集中访问设计的[5]。

这类安排会导致企业暴露于风险中，劫持类攻击可以轻松瞄准整个环节中薄弱的一环——家庭路由器和 DNS[6]。拥有高级访问许可的高管和员工更容易受到攻击。报告披露，黑客们已经开始利用家庭路由器的漏洞，使用“DNS 劫持，将用户重定向至下载新冠肺炎新闻应用软件的网页 [7]。”这种攻击可以引发更多攻击，可在重定向用户的同时植入信息和恶意软件。

企业需要确保高管、合作伙伴或客户在尝试访问企业信息时不被导向恶意内容。企业需要巩固两个领域：1. 权威 DNS 服务器和 2. 通过递归 DNS 网络（即 ISP）提供的信息。

企业的权威 DNS 服务器控制着所有在线服务的位置。如果该服务器遭到劫持，则注册商处的名称服务器记录会被更改，或者 DNS host 的 DNS 区域记录会被更改，黑客可以将所有访问企业在线服务的人重定向至他们希望的任何位置。这是一种在防火墙外发生的可怕攻击。臭名昭著的 DNSpionage[8]活动与巴西银行劫持事件[9]就是前车之鉴。

多个 ISP 和路由器也会通过递归 DNS 保存服务器位置。该架构的设计旨在改善 DNS 的解析速度和冗余。然而，这也是影响 DNS 记录的主要方式，因为企业并不能控制递归服务器，而中间环节实在是太多了。其中肯定有某一方存在着安全漏洞。

当黑客控制了任何递归 DNS，包括家庭路由器，他们就能影响企业网站（主域名）、企业 VPN（VPN 服务器）或企业邮箱（邮箱服务器）指向的位置。所有这些攻击甚至在触及防火墙前就会发生，因此必须将它们阻挡在防火墙外。

为了避免这种情况，企业应当使用 DNS 安全扩展（DNSSEC），以提供“DNS 数据与数据完整性密码鉴定[10]。”该方法由互联网名称与数字地址分配机构（ICANN[11]）和领先的安全专家[12]提出，是预防 DNS 劫持的关键方法之一。虽然 DNSSEC 无法对 DNS 数据进行加密，不能“一劳永逸”地解决 DNS 安全问题，但依然是一种关键的安全控制手段。这是唯一一种能保障 DNS 数据完整性的协议，用户可以确保从递归 DNS 服务器处获得的网站地址（A 记录）与企业发布的完全一致。

3. 去全球化引发对本地内容的青睐

另一个可能影响数字资产管理的趋势是去全球化。在过去数年中，民粹主义和去全球化成为了影响世界的重要力量。这场新冠肺炎流行病很可能加速了两者的发展。这两个趋势都引发了更强烈的民族情绪，以及对本地商品和服务的青睐[13]。这种本地倾向也可能影响网络世界，改变企业用数据资产与客户沟通的方式。

例如，跨国企业通常会使用.COM 建立一个集中的全球网站。部分本地企业喜欢使用 .COM 域名，以凸显出其具有较大的企业规模或其业务遍及全球——这可能是全球化的互联世界的体现。

近年来，使用.COM 全球网站的惯例受到了国家互联网政策的挑战。为了在各国的管辖区域内符合规范，企业必须建立不同的网站。在去全球化趋势下，这种挑战可能会延伸到政策领域之外，影响到商业倾向。消费者可能更喜欢购买本地商品。如果这确实成为了社会趋势，规模较大的跨国企业可能更需要进行本地化，重点聚焦本地内容，甚至使用与本地受众相符的国家代码顶级域名（ccTLD）。所以，相较于将 ccTLD 重定向至.COM 域名，本地化的重定向战略更容易赢得消费者的认可，因为它可以使.COM 网站根据地理方位重定向至相应 ccTLD。

数据资产是企业在网络世界中关键的识别因素之一。这包含了 IT、知识产权和品牌宣传之间的复杂联系，也会对网络安全产生深远的影响。CSC 解析了数字资产管理在新冠肺炎后世界中可能发生的变化，并展示了多个安全事件中的漏洞滥用与资产管理之间的关联。数字资产的管理是企业在线营运的关键一环，也需要高层管理者的不懈监督。

[1] qz.com/1703322/internet-pioneer-vint-cerf-on-what-we-need-to-do-to-fix-the-web/
[2] blog.mozilla.org/data/2020/03/30/opening-data-to-understand-social-distancing/
[3] nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html
[4] myhackernews.com/blog/the-wechat-scams-sweeping-asia/
[5] scmagazine.com/home/security-news/covid-19-exposes-gaps-in-cyber security-safety-net-as-millions-work-from-home/
[6] tomsguide.com/news/coronavirus-router-hack
[7] techspot.com/news/84571-home-router-dns-attack-redirects-users-malicious-covid.html
[8] krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/
[9] wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/
[10] en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
[11] icann.org/news/announcement-2019-02-22-en
[12] krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/
[13] ft.com/content/9f558874-7fe2-11e6-8e50-8ec15fb462f4

关于 CSC

CSC 是企业域名、域名系统 (DNS)、数字证书管理以及数字品牌和欺诈防御领域值得信赖的供应商，位列福布斯全球 2000 强企业和“全球最具价值 100 大品牌®”。随着全球公司加大安全性方面的投资，CSC 可以帮助他们了解存在的已知安全盲点，并帮助他们保护域名、DNS 和数字证书。CSC 的专有安全解决方案可保护公司在线资产免受网络威胁，避免重大经济损失、品牌声誉受损，或因不遵守《通用数据保护条例》（GDPR）之类的政策而受到重大经济处罚。我们还提供在线品牌保护（在线品牌监控和执行活动的结合），采用全面的数字资产保护方法，并提供欺诈防御服务来抵御网络钓鱼攻击。

请与我们联系 **cscdbs.com/cn**.