数字资产安全：

回归本质要素

数字资产安全：*回归本质要素*

全球范围内的网络攻击和数据泄露事件层出不穷，这表明形势日益紧张并且呈上升趋势，确保环境安全变得更加复杂。虽然企业不断进行技术投入，但那些力求确保组织安全的企业每天都面临挑战。

目前，许多企业已采用了各种行之有效的安全方法、工具和技术以保护环境和品牌安全，但网络攻击防不胜防。黑客、激进黑客、网络罪犯、民族国家和内部人员（例如员工）都在试探安全协议，以寻找可入侵的薄弱环节。

既已知晓数据会从各类入口点流入，在内部和边界防护存在区分的组织应立即重新审视其安全方案，特别是各种数字资产（即域名、域名系统 (DNS) 和数字证书），以确保企业日常运作顺利进行。

如何从传统的网络安全方案转型为可应对现今风险的方案？

了解并识别您的数字资产，以便对其进行适当的管理。

及时了解事件对企业的影响并制定相应的计划。

优化您的投资回报率。您需要了解投资是否具有价值（评估重要域名）。

防范来自多个数字渠道的风险。

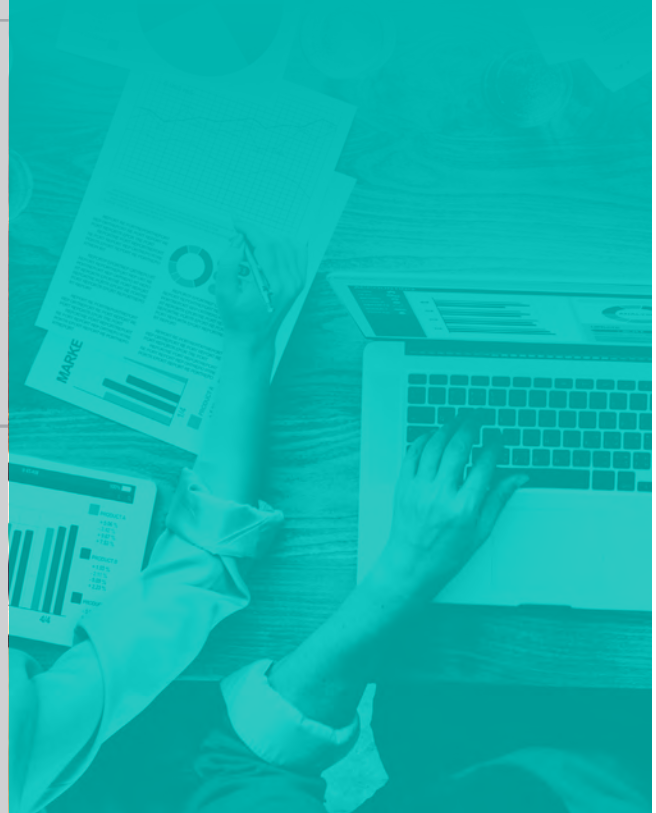
1

2

3

4

了解并识别您的数字资产，以便对其进行适当的管理。



在过去 20 年里，贵企业已积累了庞大的数字资产。这些数字资产代表着贵公司，确保企业能够开展交易，与客户、供应商和员工顺畅沟通和互动。简而言之，这些资产已转变了您的沟通、运营和消费方式。

如今，全球联系更为紧密，这是全球各地企业的绝佳机遇，但同时也伴随着挑战。全球数字经济不断发展，域名、数字证书、社交媒体用户名和移动应用程序等在线资产也在增加。因此，公司必须了解自己拥有和使用的在线资产。否则，企业会容易遭受品牌侵权和网络攻击。

企业所拥有和实际使用的完整信息可能散布在各个部门，包括市场营销、法务、IT 甚至是人力资源部，因此最佳方法是首先创建在线资产完整列表，然后请求供应商和注册机构进行审核。每家公司都应全面性看待这个问题，也就是说，假设您在美国办事处工作，也应关注公司全球业务运营所在地的在线资产。

以下是检查清单。请确定：

- ○ **您拥有的域名，包括出于推广目的注册的域名（例如虚链接）和防御原因**
- ○ **各个域名的 DNS 提供商，无论这是您的域名注册机构、专业的 DNS 提供商还是您自身提供支持的基础架构**
- ○ **您拥有的数字证书数，包括每种数字证书的验证类型以及管理方式**
- ○ **您拥有的各大平台的社交媒体帐户数量**
- ○ **有权访问社交媒体用户名和密码的人员，以及帐户管理方式**
- ○ **您是否已创建并发布了移动应用程序，以及它们的管理方式**

重要的是，在汇编此信息时，还必须了解有访问权限的人员及可访问的内容。

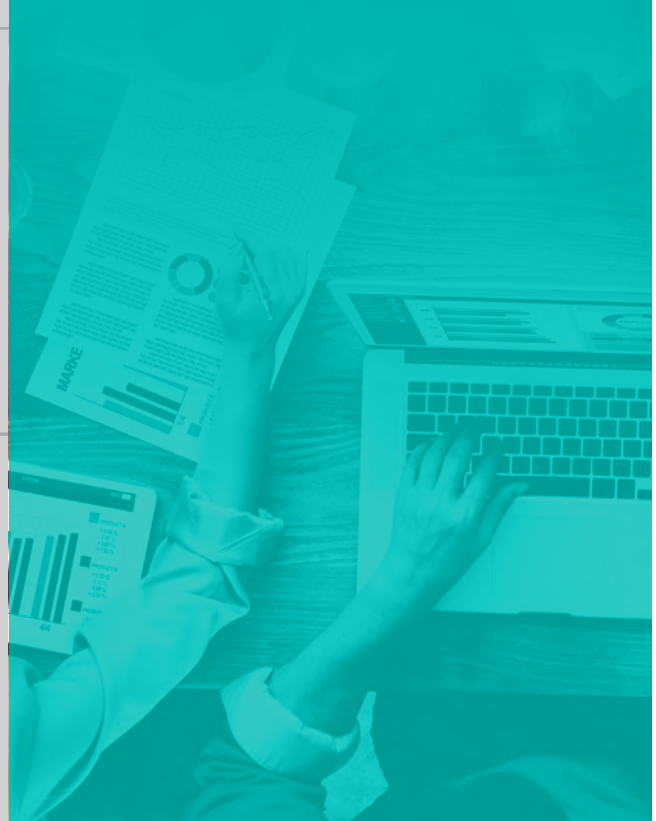
1

了解并识别您的数字资产，以便对其进行适当的管理。

2

3

4



与企业级提供商合作整合您的在线资产

了解您的全球组织在域名、DNS 和数字证书方面的需求，以确保您的所有合作提供商均符合要求。每个领域都有一系列提供商，从低成本的“DIY”提供商（有限的服务模式和基于信用卡的计费模式）到提供“白手套”服务以及提供全球化公司所需的 SLA、责任和计费模式的企业级提供商。在选择合作伙伴时，其安全状况也应是主要考虑因素。

除了仔细考量提供商的质量，最佳建议操作是整合您的在线资产，以确保顺畅的管理和业务连续性。安排专门的团队和平台（理想情况下）管理您的所有在线资产，可进一步提升您对变化的适应性，包括注册或注销域名、更改社交媒体凭证、更新数字证书等。最重要的是，您可清晰全面地了解安全漏洞情况。

要求潜在提供商或现有提供商对您的在线资产进行审核。如果您还没有完成此项工作，请与企业级提供商合作。企业级提供商更有可能提供优质的数字证书、域名和 DNS 管理。企业级提供商还应能够监视其管理的所有域名，以实施您的整合DNS 和数字证书策略。您要回答的一些问题包括：哪些域名不再使用或者未正确解析？哪些业务关键型域名未使用域名系统安全扩展 (DNSSEC)？您的业务关键型域名是否启用了“SSL 始终开启”功能？

至少应定期维护此类审计，以规范您的策略并识别未遵循该策略的注册域名。凭借优质提供商，分析将尽可能接近实时情况，并在出现潜在问题或不合规情况时向您发送通知。这意味着，您在制定需要员工遵循的政策后，还需要对员工进行培训。

详情请见第 4 点。

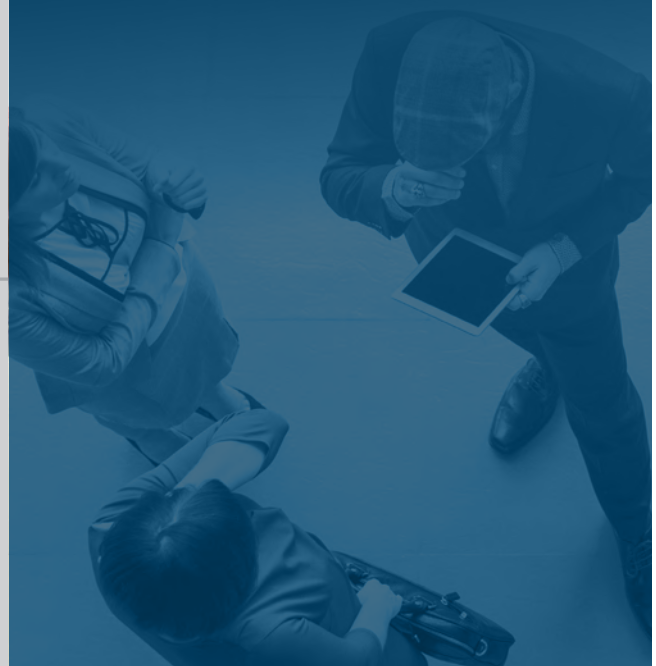
1

2

3

4

及时了解事件对企业的影响并制定相应的计划。



这样，在出现问题时，您便可重新审视局势，并将其与业务连续性相关联，进行董事会讨论，这一点很关键。

业务连续性研究所 (Business Continuity Institute) 发布的 2018 年度 **BCI 地平线扫描报告 (BCI Horizon Scan Report)**根据 76 个国家/地区 657 名受访者的报告，列出了十大业务连续性风险。可能某些人会感到惊讶，数字资产在以下四种风险中发挥了重要作用：

网络攻击。域名系统 (DNS) 容易受到各种网络攻击的影响，包括 DNS 缓存中毒、DNS 劫持、域名阴影、恶意软件、DNS 隧道、分布式拒绝服务 (DDoS) 和网络钓鱼攻击，以及利用过期数字证书等。

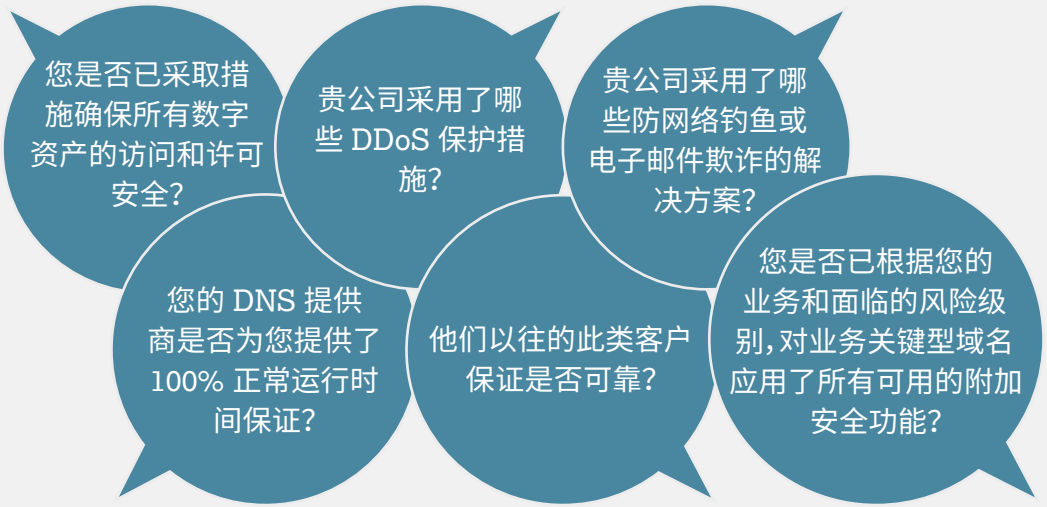
数据泄露。数字资产网络攻击越来越多地被网络罪犯用于窃取数据，或是通过掩蔽另一种攻击载体，或者直接利用资产的安全性和管理问题。

非预期 IT 和电信中断。如果公司的域名或 DNS 出现故障，则其无法通过互联网以任何方式进行通信。如果出现这种情况，组织将如何与客户和员工进行通信？

供应链中断。公司域名和 DNS 故障将会导致企业无法通信，企业应如何维护运营和供应链？

很明显，此类故障影响很大，因此必须对您的在线资产采取基本的安全措施。全球范围内的网络攻击形势日益严峻，攻击是来自激进黑客还是网络罪犯并不重要；重要的事实在于，一旦遭受网络攻击，公司将付出沉重的代价。

自查



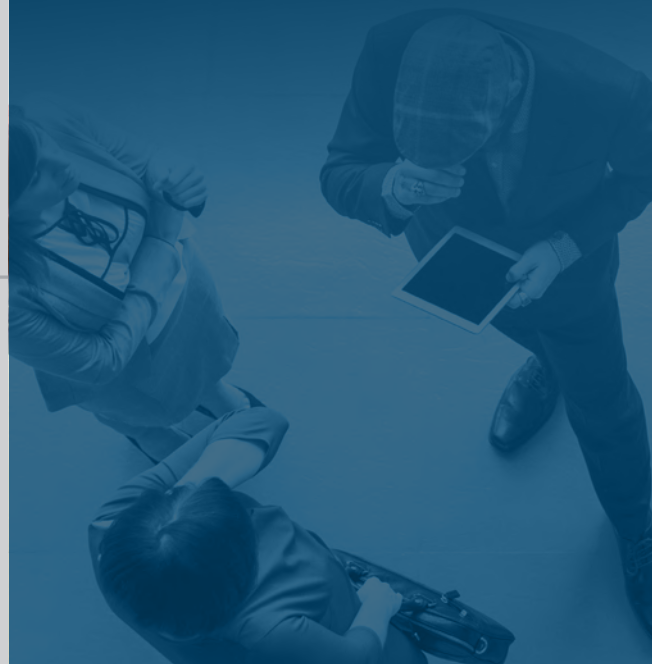
1

2

3

4

及时了解事件对企业的影响并制定相应的计划。



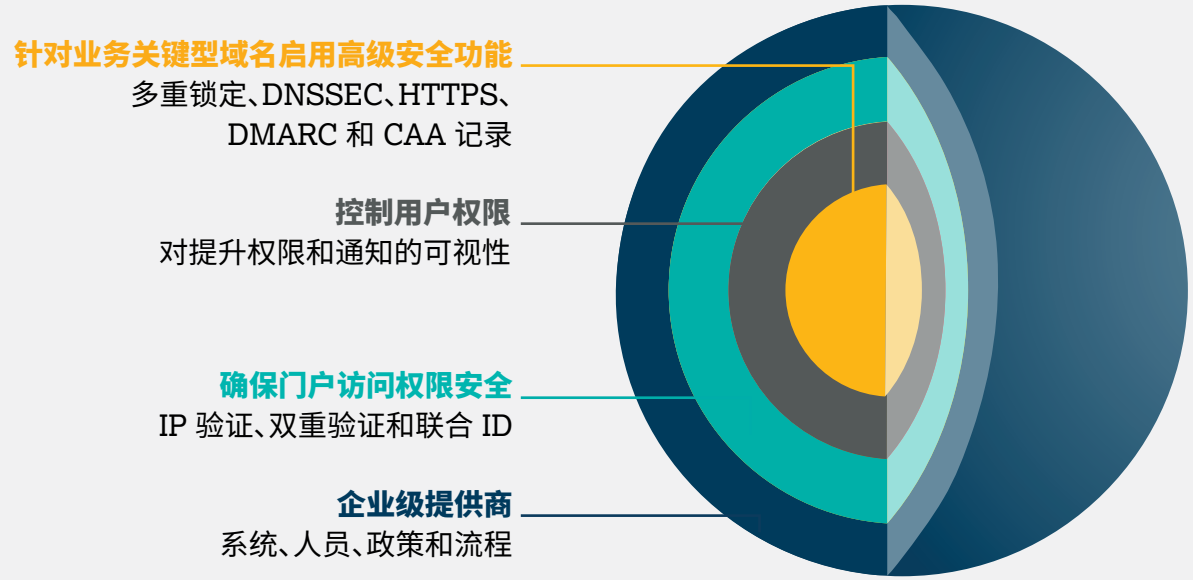
了解哪些资产属于业务关键型资产

一项重要考量在于，了解您的哪些数字资产属于业务关键型资产。这听起来很容易，但是实际上，您需要了解在全球业务中，各职能部门对域名的使用情况。

我们建议与已构建算法或正向机器学习迈进的提供商合作，以便尽可能实时地将您的业务关键型域名识别为重要资产。

采用纵深防御方案

纵深防御是一种多层安全方案理念，保护您的数字资产免受许多可能导致上述业务连续性风险的威胁。



1

2

3

4

优化您的投资回报率。您需要了解投资是否具有价值（评估*重要域名*）。

首先，数字资产（尤其是域名）的获取成本相对较低，导致投资组合庞大，投资回报率低。但是，仍有可能提升投资回报率，这一点尤其重要，因为企业需要在重要域名的高级安全功能上投入更多资金。概念很简单，放弃和剥离对您的品牌无价值的资产，以筹集其他安全投资所需的资金。

您需要确保您的数字 IP 解析为相关内容。然后，您可以评测流量，这是投资回报率的一项关键指标。您仍然可以保留不再活跃或已重定向到主域名的专项活动的域名。您可能还想查看出于防御目的而注册的域名。尽管它们可能不会吸引很多流量，但它们可能会保护您的商标免遭侵权。保留必要的防御性注册域名，并尽可能安全剥离不必要的域名，以优化您的投资组合。这样，您可以识别确定与可用域名（包括品牌）相关的缺口，并在必要时进行注册。

但是，弃用的公司域名通常包含一些活动痕迹，犯罪分子可将其用作攻击载体。因此，任何清理或资产剥离活动都应与企业级提供商一起谨慎开展。拥有可识别重要域名的工具的提供商将是最佳选择，可确保您仅清理或剥离对您没有真正价值的域名。

1

2

3

4

防范来自多个数字渠道的风险。

在您掌控自己的数字资产后，接下来应该关注利用了您的品牌或假冒您名义的第三方所拥有的资产。

对于大多数行业而言，在线监控服务是一项重要资产。您监控的程度取决于您自己的数字品牌策略，因此，您应该再次与公司的法务和营销部门合作，以帮助确定密切监控的重要对象和无需担心的问题。

您需要考虑到，您想要的是降低安全风险，而法务和营销部想要防止您的品牌被侵权。尽管动机不同，但你们拥有共同的目标，即保护公司的安全！

根据优先级安排数字品牌监控活动，让这些活动更具成本效益，增加发现最具破坏性的威胁的可能性。您可在不怀好意之人接近您的宝贵财产之前识别他们。确定了适合您品牌的监控解决方案后，您可以确定需要优先解决的警报，可忽略不会影响您品牌的警报。但是要知道，筛选监控结果会是一项持续性工作。

监控还让您能够维护安全策略和控制措施。首先要确保所有员工都通过您选择的集中式域名管理合作伙伴注册域名。然后，请务必查看相关的 DNS 和数字证书，确定该域名是否重要，以及是否已根据该域名对您品牌的重要性适当启用了安全功能。

合格的品牌监控服务提供商可帮助您管理持续攻击；优秀的提供商甚至可为您筛选警报，仅向您提供需要关注的最重要的侵权行为。

CSC Security Center

CSC Security Center℠ 可满足先前无法实现的行业需求，对业务关键型域名进行全面的安全监管。这款独一无二的解决方案使用 CSC 专有的高级算法创建，是市场上非常全面的域名安全解决方案。该解决方案可识别重要域名、监视持续威胁、在出现变更时发送通知并精简威胁防御工作。我们真诚希望您更深入了解CSC Security Center的功能与优势，以及它转变您的数字资产管理的方式并减少网络风险。

cscdigitalbrand.services