CSC

# 超越防火墙的措施：

*通过实施DNS防护*
*减少在线漏洞和威胁*

# 超越防火墙的措施：
# 通过实施DNS防护减少在线漏洞和威胁

25年来，防火墙一直是网络安全的第一道防线。防火墙在安全、受信和内部网络与外部不可信赖的网络控制（例如：互联网）之间建立了屏障。

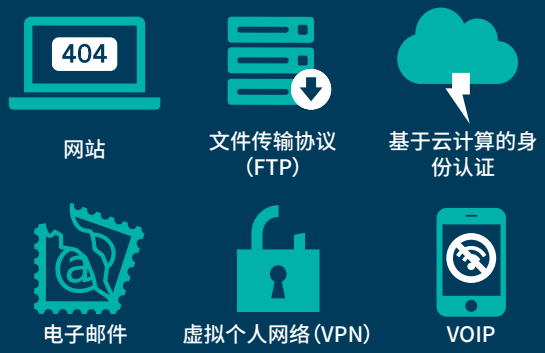
由于网络犯罪无处不在并不断滋生，我们需要防火墙。IT安全领域的业界人士通过加强防火墙的防护功能并进行模拟和渗透测试应对网络犯罪现象。

**但是，如今网络犯罪处于白热化阶段，仅靠防火墙力度不够。**

企业往往会忽视数字资产的安全性，因为数字资产不受防火墙保护 —— 我们将数字资产定义为域名、域名系统（DNS）和数字证书。妥善管理数字资产（尤其是DNS）对业务的顺利开展至关重要。

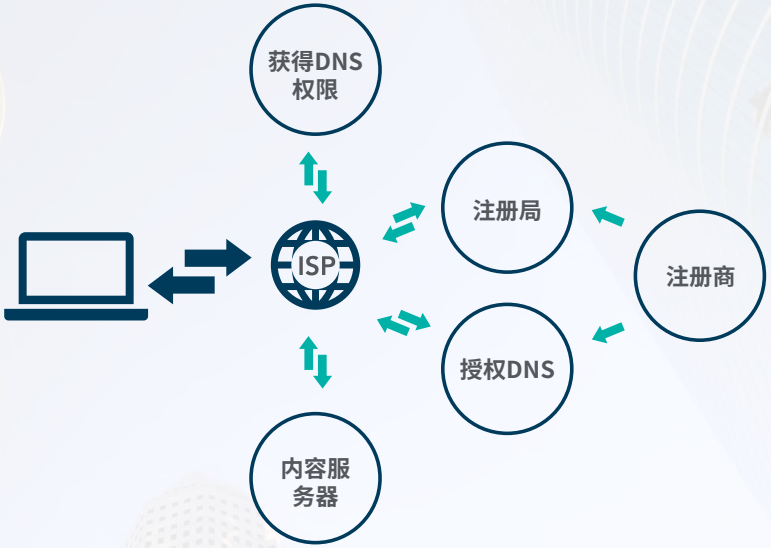
DNS构成互联网运作方式的基础设施，旨在将用户导向正确的网络内容目录。当DNS发生故障时，网站也会发生故障。一旦发生该情况，按常理只有通过电话和电子邮件保持业务运转。但是，DNS故障意味着电子邮件、电话（VoIP）和员工远程登录功能全部无法运转。移动大型数据集的文件传输协议和各种多重身份验证服务（例如：电子邮件、Google®和Microsoft®）也会失效。

数字资产的故障会产生重大影响，例如：收入损失、数据丢失和品牌声誉受损。




## DNS易受损；需谨慎处置！

看似简单的首字母缩写词 —— DNS，掩盖了系统的复杂性，因为该系统由分散在全世界范围并在信息交换传递过程中运行的独立实体组成。由于系统的复杂性，DNS面临多个潜在故障点，因为系统中的每个故障点都容易受到攻击，从而对您的组织产生负面影响。




## 与DNS漏洞相关的10大威胁和风险

1. DNS劫持
2. DNS缓存中毒
3. 域名屏蔽
4. DNS中断
5. 恶意软件
6. DNS隧道
7. 零时差攻击
8. DDoS攻击
9. 域名到期、被盗或丢失
10. 数字证书到期、丢失或安装不当

1

2

3

4

## 四步深度防御法

深度防御是指可在防火墙外部保护您的数字资产的多层次安全方法。

# 第1步：
# 采用高级安全防护措施。

对于您的关键业务域名，即支撑您的业务运营的域名，您可添加：

- 注册锁以阻止DNS劫持
- 域名系统安全扩展（DNSSEC）以阻止DNS缓存中毒
- 数字证书以对数据进行加密
- 基于域的消息验证、报告和一致性（DMARC）以对您的电子邮件进行身份验证并减轻员工受到的网络钓鱼攻击威胁
- 证书颁发机构授权（CAA）记录以强制执行您的数字证书政策

1

2

3

4

## 四步深度防御法

深度防御是指可在防火墙外部保护您的数字资产的多层次安全方法。

# 第2步：

# 控制用户权限。

确保您拥有访问关键业务资产的人员名单，访问者拥有的权限，并主动管理该等权限。在同一平台上点击按钮查看访问权限、接收通知、查看变更内容并对任何变更授予权限。这将有助于管理未授权变更，例如：DNS劫持和域名屏蔽。

1

2

3

4

## 四步深度防御法

深度防御是指可在防火墙外部保护您的数字资产的多层次安全方法。

# 第3步：

# 确保门户网站访问的安全性。

您应确保正在使用的所有门户网站权限的安全性；每个门户网站在授予访问权限时采用多重身份验证，包括：IP验证、双重身份验证和联合ID（或单点登录）。本步骤还有助于整合供应商，管理访问权限，并减少他人擅自更改您的数字资产的风险。


## 四步深度防御法

深度防御是指可在防火墙外部保护您的数字资产的多层次安全方法。

# 第4步：
# 雇用企业级供应商。

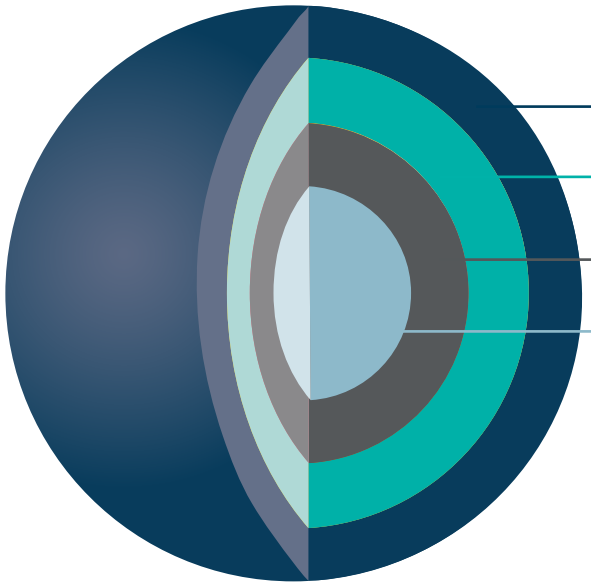
最后，慎重选择您的合作伙伴。除了限制您用于控制威胁因素的供应商和门户网站的数量，在域名、DNS或数字证书管理的质量上不可轻易妥协。可通过优质企业供应商以安全系统和流程统一管理所有资产，以缓解风险和威胁。企业供应商具备内部分析师的专业知识，并从战略客户经理处汲取知识和获得支持，以助您了解风险并选择正确的解决方案。

## 如何了解防火墙外部的安全威胁

在CSC，我们发现市场上尚未推出可帮助企业，尤其是首席信息安全官，判断资产在防火墙外部情况的产品。现有仪表板专注于消除内部网络和防火墙的差距，可用于披露防火墙范围之外重大风险的工具少之又少。

CSC Security Center℠旨在帮助IT专业人员减轻未受保护数字资产的风险。使用专有算法，我们能够通过检查与域名有关的多个特征和了解相互关联的关系，预测域名组合中的哪些域名至关重要。通过对域名的进一步检查识别是否存在任何风险，并提出减轻威胁的建议。

## 了解风险才能采取有效的控制措施和策略



随着CSC Security Center的发展，公司如今可识别重要域名和安全盲点，包括：DNS缓存中毒、域和DNS劫持、DDoS攻击等引起的风险。我们建议您进一步采取措施，落实适当的政策，并建立加强公司安全态势的正确制度。

### 企业类供应商

- 通过ISO 27001认证的数据中心
- SOC 2®合规
- 第三方渗透、漏洞测试、安全测试
- ICANN和注册管理机构认证
- 一流的DNS和数字证书合作伙伴
- 安全第一，网络钓鱼意识培养和社会工程培训
- 强制性的明确办公桌政策
- 强制性书面要求（绝不通过电话进行）
- 数据和GDPR合规（例如：WHOIS规范）
- 账户信用支持的自动续订政策
- 注册局转移锁定政策

### 确保门户网站访问的安全性

- 强制性双重身份验证政策
- 免费IP验证
- 免费联合ID

### 控制用户权限

- 对域名升级设置通知提示
- 授权联系政策

### 先进的安全功能

- 重要域名识别
- 安全盲点检测
- 自动锁定政策

DNS劫持攻击在网络安全中占据核心地位，在每日头条报道中，2019年成为分水岭。

- CSC提醒公司注意：DNS劫持事件增加
- DNS劫持影响了客户对核心互联网服务的信任
- 与已发布的域名系统攻击报告有关的警报
- 紧急指令19-01避免篡改DNS基础设施

一场出于以下目的，针对国家安全组织、外交部和著名能源组织的全球行动已经确定：首先针对第三方实体（例如：DNS注册商、电信公司和互联网服务供应商）修改DNS名称记录，以将用户导向参与者控制的服务器；其次窃取组织的合法数字证书，以在参与者控制的服务器上使用。

CSC安全服务产品总监Mark Flegg表示："犯罪分子通过DNS攻击将网络流量从合法站点导向非法站点，使客户和公司面临巨大风险。""最近的复杂和恶性攻击利用许多公司曾经设置但忽视的DNS基础设施的弱点。我们强烈建议客户利用现有工具和建议确保其数字基础设施的安全。"

攻击的严重性导致多个政府和国际组织对指令和警报作出响应，这在域名安全中是前所未有的现象。

CSC 数字品牌服务总经理Mark Calandra表示："域名和DNS劫持安全威胁并非近期才出现，因此，我们研发了CSC Security Center，并鼓励全球成百上千的大型公司使用CSC Security Center保护其赖以运行的在线关键要素。""最近一轮布局精密的攻击造成的影响敲响了警钟：有效管理域名、DNS和数字证书对提高任何在线运营的公司安全状况至关重要。"

如欲了解有关DNS劫持风险的更多信息以及如何最好地缓解威胁，请阅读我们的博客 ***对域名锁一知半解？了解其复杂性和安全性*。***

* 仅用英语

## 每个组织应对重要域名实施的四大关键政策：

**强制性多重身份验证，以控制用户访问权限**

**自动续订政策，以防止域名到期和丢失**

**自动锁定政策，以防止他人擅自变更域名**

**确定证书颁发机构的数字证书政策**

数字资产管理不仅仅是管理域名续订、修改和数字证书替换。我们坚持使用创新技术并结合行业领先服务，积极帮助客户实施和规范其政策。我们旨在防止客户业务受到防火墙外部的威胁。

如欲了解有关域名安全基本要素的更多信息，请参阅 **"数字资产安全：回归根本！"** 白皮书。

cscdigitalbrand.services/cn