长期实施业务连续性计划的五个安全盲点

长期实施业务连续性计划的五个安全盲点

作者：Alban Kwan，东亚区域总监

新型冠状病毒 (COVID-19) 的爆发促使中国大陆与香港的许多组织实施业务连续性计划 (BCP)。上一次在 2003 年爆发的非典疫情持续了九个月，感染率快速上升，而这次的新兴冠状病毒很可能导致业务长期中断，使得企业严重依靠业务连续性计划。

BCP 中最常见的举措是使用 VPN 实现安全的远程访问，从而使员工能够在家办公。尽管 VPN 早已广泛用于商业，但此次疫情导致感染区域内的远程访问量长期大幅激增，而这可能导致企业面临不可预见的风险。本文将讨论可能出现的若干安全盲点。

1. VPN 劫持

在 2019 年 12 月，发现了一种新 VPN 漏洞 – CVE-2019-14899[1]，亚马逊的工程师 Colm MacCárthaigh 称该漏洞“极其聪明”且“非常厉害”。该漏洞可攻击多种不同的 VPN，因此“使用哪种 VPN 技术似乎并不重要”[2]。该漏洞是 TCP 序列号猜测攻击的变异，攻击者利用各种技术观察与确定 TCP 序列号，以伺机插入恶意数据包与有效劫持 VPN 隧道。

这种类型的攻击在有针对性的劫持活动中非常有效，适用于任何设备与 VPN，使用未加密家庭无线网络访问 VPN 的无戒备心的员工易被攻击。

开发了亚马逊云服务的 VPN 产品，其警告，要是与 **DNS 欺骗**[3] 联用，该攻击会构成更加严重的威胁。攻击者很容易根据数据包的大小和位置分析 DNS 请求并给出回复；DNS 通常是序列中的第一个流量，而且 DNS 查询在 VPN 建立之前发生。因此，“通过 DNS 劫持流量通常比有效负载注入更有效”[4]，可用作 VPN 劫持攻击的一部分。攻击者也可通过该攻击的变异盗取 VPN 密码，从而自由访问公司网络。

[1] seclists.org/oss-sec/2019/q4/122
[2] zdnet.com/article/new-vulnerability-lets-attackers-sniff-or-hijack-vpn-connections/
[3] openwall.com/lists/oss-security/2019/12/05/3
[4] openwall.com/lists/oss-security/2019/12/05/3

2. 通过 DNS 劫持盗取 VPN 密码

在 2019 年“海龟”攻击者发起的著名 DNS 劫持活动中，Cisco Talos 报导犯罪者能够盗取电子邮件和其它登录凭证，以及将所有电子邮件和 VPN 流量转发到攻击者控制的伪服务器。

攻击者通过劫持域名注册商或 DNS 服务供应商访问受害组织的关键业务域。劫持到域名后，攻击者会获得目标域的 SSL/TLS 数字证书（如 vpn.victimcompany.com），从而“破解拦截的电子邮件和 VPN 凭证的密码，直接查看明文”。[5]

从 DNS 劫持数量以及在这之后被攻击的知名注册商数量的增加来看，其他黑客已重现“海龟”攻击。这种趋势很可能持续存在，因为相比于攻击受防护墙保护的任何对象，劫持 DNS 的成本效益更高。

3. 域名与 DNS 安全性可能影响 VPN

既可利用 IP 地址直接设置 VPN，也可通过 DNS 设置 VPN。使用 DNS 设置 VPN 这一方法更加灵活，因此更为常用。使用这种方法时，以上讨论的域名和 DNS 劫持问题会造成另一维度的风险。为降低这些风险，公司应评审注册商与 DNS 的安全性。

i. **注册商安全性** – 在盗用您在注册商处的账户后，攻击者会获得您的域名注册商保存的将域名与您的 DNS 相链接的域名服务器记录的控制权，从而将您的核心域转发至任何 DNS，实现所有类型的中间人攻击。注册商泄漏**完全发生在您的防火墙之外**，必须通过适当的第三方风险管理予以规避。有效的降险策略包括：

   a. 使用企业级服务供应商。避免使用曾存在安全漏洞、安全级别和成本低的服务供应商。
   b. 确保您的注册商提供注册局锁定服务且启用 DNSSEC。
   c. 确保您的注册商登录门户采用适当的双重身份验证(2FA)。如可能，避免采用基于 SMS 的 2FA。
   d. 锁定您在注册局的重要域（请勿与注册商锁定混淆）。

值得注意的是，VPN 连接背后的域可能与核心域不同。内部使用的域名可能被忽视，而不被视为需要适当的关注与安全性控制的重要域。这些域可能在安全时期被视为不太重要的域，或这些域可能由前员工或承包商设置，造成现任网络工程师无法全面查看这些域。我们强烈建议您开展内部审核，以检

[5] csoonline.com/article/3500492/widespread-dns-hijacking-attacks-steal-target-s-vpn-credentials.html and krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

查用于内部重要系统（尤其是 BCP 相关服务）的任何域，以及确保适当的安全控制。一旦这些域被劫持，您的 BCP 将中断。

ii. **DNS 安全性与可用性** – 攻击者还可直接劫持 DNS 服务器。只要您的 VPN 连接使用 DNS，注册商泄漏或 DNS 劫持就可能导致您的 BCP 完全停止。以下列举了若干用于规避 DNS 劫持的最佳惯例:

   a. 使用企业级服务。避免使用成本和安全性低的 DNS 服务，尤其是免费 DNS 服务。
   b. 确保您的 DNS 登录门户采用适当的 2FA。应避免基于 SMS 的 2FA。
   c. 确保您的 DNS 服务供应商提供全天候（一天 24 小时，每周 7 天）的支持且能够通过系统连接。如果服务要求您记录权证与手动更新区域，则在紧急情况下的风险会过高。
   d. 监控 DNS 区域文件的变化。尽管能够在 DNS 劫持中防止未经授权人士修改您在 WHOIS 中的域名服务器记录，但注册局-注册商锁定不会锁定区域。与能够监控您的 SIEM 或在您的 SIEM 中集成监控服务的服务供应商合作。

请参阅 **加强 DNS 安全性的 6 种方法**，了解与 DNS 保护相关的更多信息。

4. SSL VPN 与数字证书管理风险

VPN 可通过 IPSec 或 SSL 加密。由于易于实施、成本低且可扩展性高，SSL VPN 更受青睐。鉴于没有许可与难以在大规模实施 BCP 的情况下实施 IPSec VPN 系统，公司可能针对远程员工实施 SSL VPN。

在这种情况下，考虑与数字证书管理相关的风险至关重要，这些风险通常来源于坏习惯。不幸的是，即使是像 LinkedIn 这样的大型组织，管理不善也时有发生，给企业造成重大损失（示例 1, 示例 2, 示例 3）。

如果在 BCP 过程中实施 SSL VPN，您的组织需审核政策，确保证书未到期。以下列举了若干最佳惯例:

i. 如果您的组织使用大量数字证书，可考虑使用数字证书管理服务，实现内外部证书的自动更新与安装。
ii. 如果未首选自动更新，则始终会出现未注意到数字证书到期的情况，就如墨菲定律所言，会出错的，终将出错。您的供应商对事件快速响应的能力至关重要。供应商应提供全天候（一天 24 小时，每周 7 天）的支持，最好不是“仅在线提供支持” 以及仅可通过网络访问的供应商。
iii. 实施有助于为您的数字证书创建治理框架的 CAA（证书颁发机构授权)记录，以便防止向您的域错误签发 SSL 以及防止员工购买到未获授权的证书。

5. 突发事件中的网络钓鱼攻击

总会有网络罪犯伺机利用任何突发事件，这是极其不幸的事实。“随着人们越来越担心武汉冠状病毒...网络罪犯发送自称含安全保护措施建议的网络钓鱼邮件，利用人们的恐惧心理。这类电子邮件已在美国和英国出现”。[6]

至今，CSC 已检测到 63 个含“corona（冠状）”的注册域，涵盖的范围从信息位点、销售口罩的电子商务网站到提供特定品牌机器精选采购建议的信息网站。与医疗用品或医药相关的公司需了解，造假者可能利用网络钓鱼活动促销伪劣产品，无论产品实际是否与冠状病毒有关。

另一方面，由于容易被抗病毒软件识别，网络钓鱼者不太可能在邮件和域名中使用病毒名，但他们会利用品牌诱使受害者阅读启用宏的 word 报告或被病毒感染的 pdf 报告，从而感染受害者的机器。公司需意识到公司品牌是网络钓鱼者使用的潜在手段，公司客户会因此成为受害者，公司品牌也会因此受损。

网络钓鱼者可通过鱼叉式网络钓鱼、捕鲸或对执行主管和员工实施商务电子邮件入侵(BEC)从内部攻击您的公司，也可通过在某域或品牌欺诈网络钓鱼活动中使用您的品牌名，从外部攻击您的客户。信息安全团队应检测这类攻击。

对于以聚焦于内部的网络钓鱼，建议实施 DMARC 协议，以控制 SPF 记录设置的电子邮件拒收政策。您应确保您的电子邮件网关支持 DMARC，从而确保有效滤除谎称是您的员工或合作伙伴的欺诈性电子邮件。

对于聚焦于外部的网络钓鱼，建议您实施防欺诈监控服务。这是保护无复杂防火墙与电子邮件网关的客户的唯一方法。

BCP 用于确保业务在危机期照常运营，但如果使用的系统（如 VPN 和防火墙外的 DNS、域和数字证书）有风险，BCP 会导致组织出现安全漏洞。意识到安全盲点，确保实施正确的安全控制和政策，可降低业务连续性风险。

[6] darkreading.com/endpoint/coronavirus-phishing-attack-infects-us-uk-inboxes/d/d-id/1336946

关于 CSC

CSC 可以查找域名、DNS 和数字证书等基础互联网资产内部存在的盲点，为在网络安全领域进行重大投资的公司提供支持。CSC 独有的安全解决方案可保护公司的数字资产免受网络威胁，帮助它们避免难以承受的收入损失、品牌声誉受损，或者因为违反欧盟通用数据保护条例（GDPR）这样的政策法规而受到严厉的经济处罚。除了互联网资产，CSC还保护被冒牌网站、网络欺诈和IP违例等行为所侵犯的在线品牌，帮助监控和消减这些攻击行为，提供执行和咨询服务以保护众多全球主流品牌。

请与我们联系 **cscdigitalbrand.services**.