选举无中断降低拒绝服务风险指南

概述

本指南为选举官员和选举技术提供商提供了积极的应对措施，以降低拒绝服务 (DoS) 事件（包括分布式拒绝服务 (DDoS) 攻击和非恶意服务中断）发生的可能性和影响。

选举官员及其私营部门合作伙伴越来越依赖网站、网络应用程序和其他网络连接系统向选民提供信息和服务。选举办公室网站和网络应用程序经常受到大量互联网流量的影响，可能会继续成为那些试图破坏或削弱公众对美国选举信心的网络威胁攻击者的吸引目标。在 2022 年中期选举期间，多个州和地方选举办公室就遭遇了 DDoS 攻击和非恶意服务中断而导致的临时网站崩溃。

在选举中，DoS 事件可能导致选举办公室网站、网络应用程序或其他依赖互联网的系统暂时无法访问，从而可能影响选民无法接收官方选举信息或使用在线选举服务（例如，检查选民登记状态和投票站信息、查看样票、申请邮寄/缺席选票、登记投票等）。这可能包括在选举周期的关键时刻重要系统（如选民登记截止日期临近时在线选民登记门户网站或选举日的投票站查询工具）的可用性中断。无论是由 DDoS 攻击还是非恶意服务中断造成的此类系统中断，都可能为外国威胁攻击者提供机会，通过诸如制造或放大有关选举网站崩溃的虚假或夸大说法，来传播虚假信息并试图削弱公众对美国选举的信心。

DoS 和 DDoS

当合法用户无法访问信息系统、设备或其他网络资源时，就会发生拒绝服务 (DoS) 事件。受影响的服务可能包括电子邮件、网站、在线账户（如银行业务）或依赖于受影响计算机或网络的其他服务。通过向目标主机或网络发送大量流量，直到目标无法响应或崩溃，从而阻止合法用户访问来实现，达成 DoS 状态。发生 DoS 事件可能是由于非恶意原因（如大量合法互联网流量导致网站宕机）或是网络威胁攻击者的行为所引起。

当过载流量来自多台协同工作的攻击机器时，DoS 事件被归类为分布式拒绝服务 (DDoS) 攻击。DDoS 攻击者通常利用僵尸网络（一组被劫持的互联网连接设备）来进行大规模攻击，从目标实体的角度来看，这些攻击似乎来自许多不同的攻击者。

可能会遭遇 DoS 事件的系统

面向公众的服务

- 选民或选举信息网站
- 选举夜报告网站
- 在线服务（如选民信息查询、投票站查询、选民登记、邮寄/缺席选票申请、候选人备案等）

依赖互联网的办公系统

- 电子选民名册
- 业务处理系统（人力资源、统计、电话线）
- 电子邮件应用程序
- 互联网语音协议 (VOIP) 电话系统

非恶意服务中断

每个选举周期，全国各地的管辖区都会因互联网带宽有限、配置错误或与规划或执行不足相关的其他原因而经历非恶意服务中断。通常，高网络流量可能会使系统不堪重负，导致其暂时无法使用。还应注意的是，其他非恶意事件（如天气事件或施工事故导致电话线、电缆或光纤线路被切断）可能会导致网站或系统宕机，这看似是 DDoS 攻击，但实际上并不是。

IT 至关重要的日期

选举日程表上的重要日期和事件会导致选举网站和在线服务的流量增加。如果管辖区准备不足，流量增加可能会导致服务中断。需要牢记的重要日期和活动包括：

- 全国选民登记日
- 选民登记运动、竞选活动和截止日期
- 邮寄/缺席选票申请截止日期
- 提前现场投票日期
- 选举日投票时间
- 结果报告

做好应对 DOS 事件的准备

选举官员和选举技术提供商可以采取积极措施降低发生 DoS 事件的可能性和影响。

与服务提供商协调

降低潜在 DoS 事件相关风险的关键第一步是：选举官员在事件发生前审查现有合同，并与网站服务提供商和互联网服务提供商进行协调。这样可确保选举官员知道在发生事件时应与谁联系，同时了解其服务提供商可能已采取的保护措施。

其次，选举官员还应确定有哪些额外的 DoS 缓解和冗余措施可供采用。大多数主要服务提供商都提供各种保护措施，基本服务可能免费提供，而高级服务则可能需要支付额外费用。CISA 保护选举的网络安全工具包和资源包含一系列由 CISA、CISA 联合网络防御协作组织 (Joint Cyber Defense Collaborative, JCDC) 成员以及网络安全社区其他人提供的免费工具、服务和资源，选举官员可以使用其来防范 DoS 事件。

最后，选举官员还应提前与所有服务提供商（网站服务提供商、互联网服务提供商和 DoS 保护服务提供商）进行协调，共享有关重要选举日期和地点等信息，要求其在关键时期提供充分的故障排除服务，并确保相互了解可能影响选举行动的任何计划性维护。

监控您的网站和活动

检测和识别 DoS 事件的最佳方法是通过网络流量监控和分析。可以通过防火墙或入侵检测系统监控网络流量。管理员甚至可以设置规则，在检测到异常流量负载时发出警报，并识别流量来源和符合某些标准的丢弃网络数据包。

选举官员应与其服务提供商合作，更好地了解他们已经监控的活动及其网站的“正常”流量是什么样。除了与服务提供商协调之外，选举官员还可以直接在自己的系统上查看某些指标，这些指标可能表明存在潜在的 DoS 事件。如上所述，能否成功识别非寻常、意外或异常活动取决于对每个系统或服务“正常”基线状况的了解。

这些指标可能包括：

- 网络性能异常缓慢（例如打开文件或访问网站速度慢）
- 特定网站不可用
- 无法访问任何网站
- 应用性能欠佳
- 处理器和内存使用率过高
- 网络流量异常高

做好应对 DOS 事件的准备

灵活的流程对于选举行动（网络行动）成功至关重要。这意味着要合理制定并实施组织网络事件响应和通信计划，其中包括应对 DoS 事件和降低其影响。

识别问题

如果选举官员评估可能正在发生 DoS 事件，则应联系其网络管理员确认中断是否因维护或内部网络问题所引起。网络管理员还可以监控网络流量，确认事件和识别来源，以及通过应用防火墙规则和可能通过 DoS 保护服务重新路由流量来并缓解情况。

在联系网络管理员后，选举官员可能需要联系其网站服务提供商，询问他们的网络端是否出现了故障，甚至询问他们的网络是否是攻击目标以及网站是否是间接受害者。在这种情况下，网站服务提供商可能会建议采取适当的行动。如果服务中断发生在关键的选举期间或需要一些时间来修复，选举官员应准备实施应急计划或行动连续性计划，使用备用或替代方案，直到正常服务恢复到可接受的水平。

在受到攻击时，选举官员也应重视网络上的其他主机、资产或服务。攻击者可能会进行 DDoS 攻击以转移对其预定目标的注意力，并借此机会对网络中的其他服务展开二次攻击。

CISA 建议选举官员和选举技术提供商应即时向以下机构报告可疑的网络攻击：

- CISA，发送电子邮件至 report@cisa.gov 或致电 (888) 282-0870
- 联邦调查局 (FBI)，通过适当的地方 FBI 办事处
- EI-ISAC，发送电子邮件至 SOC@cisecurity.org 或致电 866-787-4722
- 相关管辖区的其他州或地方当局

准备共享信息的替代方法

成功的选举行动需要随机应变。这意味着要合理制定并实施应急计划或行动连续性计划，其中包括应对 DoS 事件。

遭遇 DoS 事件的选举办公室可能无法与公众、其他选举办公室、甚至同一栋大楼内的其他办公室进行通信。在每次选举前，选举官员还应准备传播选举信息（包括非官方选举结果）的备用方法，以防 DoS 事件导致网站或其他应用程序无法使用。这可以通过多种方式实现。州或地方管辖区能够在完全独立于主网站的基础设施上托管一个备份网站，这也可以在系统维护或升级期间为各办公室提供帮助。拥有选举夜报告网站的选举办公室也可考虑将 PDF 格式的结果上传到其主网站及其州或地方网络的其他网站上。最后，鼓励选举办公室与媒体机构建立关系，以防在发生事件时能够帮助传递信息，如正确的投票站信息或非官方选举结果。

针对 DoS 事件制定内部通信计划

在制定事件响应计划的同时，选举官员应将 DDoS 攻击和非恶意服务中断纳入其通信计划。通信计划应确定一个危机通信团队（包括 IT 和通信团队的成员），规定各自的角色和职责，并建立事故期间维护通信渠道的程序。危机通信团队应做好准备，在无法访问主要办公网络或移动电话的情况下保持通信。选举官员还可以考虑准备一份与 DoS 事件相关的关键术语和定义清单，供所有工作人员使用。

选举官员还应考虑编写在 DoS 事件期间可根据需要调整和使用的临时性声明。临时性声明不仅应提供给高级工作人员和通信官员，还应提供给接听电话和接受公众与媒体提问的一线工作人员。

针对 DOS 事件的计划与培训

如上所述，选举官员应将 DoS 事件方案纳入其应急计划、行动连续性计划、事件响应计划和恢复计划中。这些计划应指导组织识别事件、缓解其影响并快速从此类事件中恢复，以及在整个事件响应和恢复过程中保持有效的通信。CISA 的《选举安全网络事件检测和通知计划指南》(Cyber Incident Detection and Notification Planning Guide for Election Security)可帮助组织制定事件响应计划。

与其他网络事件一样，DoS 事件的应对计划应明确指出所有利益相关方的角色和责任，包括组织领导者和服务提供商。该计划至少应概述确认事件、了解事件性质、部署缓解措施、监控有效性和恢复工作的程序。

DoS 事件的应对计划还应考虑行动的连续性和灾难恢复程序，尤其是在内部通信渠道受到中断影响的情况下（如无法访问网络电话系统）。组织领导层应熟悉备用或替代通信渠道，以便快速有效地联系工作人员、服务提供商或选民，例如电话树、备用电子邮件或紧急通知系统。

事件发生后，一旦服务恢复，选举官员应进行事件总结，讨论从实施事件响应和通信计划中吸取的经验教训，并相应更新程序。

最后，所有工作人员都应接受培训并定期进行事件响应演练。选举官员可以考虑将 DoS 事件纳入桌面演练或其他基于场景的培训中。例行演练至关重要，可确保所有人了解其在事件中的角色和职责，有助于发现响应计划中的漏洞，使利益相关者能够练习真实事件的紧迫性和节奏，并建立对计划和缓解措施的信心。CISA 的选举网络桌面演练(Elections Cyber Tabletop in a Box) 资源将 DDoS 攻击作为演练场景的一部分。CISA 的地区网络安全顾问 (CSA) 也可以提供评估和保护资源，包括对 DoS 事件的风险管理指导。

其他资源

整个文件及以下链接中包含的其他资源是对本指南中所提供信息的补充。鼓励选举官员和选举技术提供商查看这些资源，以做好进一步准备和降低与潜在 DoS 事件相关的风险。

- CISA FBI MS-ISAC 了解和应对分布式拒绝服务攻击
- CISA 了解拒绝服务攻击
- CISA 保护选举的网络安全工具包和资源
- CISA 分布式拒绝服务 (DDoS) 快速指南
- CISA 选举安全网络事件检测和通知计划指南
- CISA 选举网络桌面演练
- CISA 能力增强指南：针对 Web 服务的容量 DDoS 技术指南