선거 시 다운타임 방지: 서비스 거부 위험 완화 가이드

개요

이 가이드에서는 선거 관리 공무원과 선거 기술 제공업체에서 분산 서비스 거부(DDoS) 공격 및 비악의적인 서비스 중단을 포함한 서비스 거부(DoS) 사고의 가능성과 영향을 줄이기 위한 사전 예방 차원의 조치를 안내합니다.

선거 관리 공무원은 민간 부문 파트너는 유권자에게 정보를 제공하고 서비스를 제공하기 위해 웹사이트, 웹 애플리케이션, 기타 네트워크 연결 시스템에 점점 더 의존하고 있습니다. 선거 관리 사무소 웹사이트와 웹 애플리케이션에서는 대량의 인터넷 트래픽이 발생하는 경우가 많으며, 미국 선거에 대한 신뢰를 방해하거나 약화시키려는 사이버 위협 행위자들에게 매력적인 표적이 될 수 있습니다. 여러 주 및 지역 선거 사무소에서는 2022년 중간 선거 주기 동안 DDoS 공격과 악의적이지 않은 서비스 중단으로 인해 일시적인 웹사이트 중단을 경험했습니다.

선거에서 DoS 사고로 인해 선거 관리 사무소 웹사이트, 웹 애플리케이션, 기타 인터넷에 의존하는 시스템에 일시적으로 액세스할 수 없게 되면 유권자가 공식 선거 정보를 수신하거나 온라인 선거 서비스(예: 유권자 등록 상태 및 투표소 정보 확인, 견본 투표용지 보기, 우편/부재자 투표 신청, 유권자 등록 등)를 이용하는 데 영향이 미칠 수 있습니다. 이러한 상황에는 유권자 등록 마감일에 가까운 온라인 유권자 등록 포털, 선거 당일 투표소 조회 도구 등 중요한 시스템의 가용성이 선거 주기의 중요한 순간에 중단되는 경우가 포함될 수 있습니다. DDoS 공격으로 인한 것이든, 악의적이지 않은 서비스 중단으로 인한 것이든, 이러한 중단 때문에 해외 위협 행위자가 허위 정보를 유포하고 선거 웹사이트 중단에 대한 허위 주장이나 과장된 주장을 하거나 증폭시켜 미국 선거에 대한 대중의 신뢰를 훼손할 기회가 제공될 수도 있습니다.

DoS 및 DDoS

서비스 거부(DoS) 사고는 정상적인 사용자가 정보 시스템, 장치, 기타 네트워크 리소스에 액세스할 수 없을 때 발생합니다. 영향을 받는 서비스에는 이메일, 웹사이트, 온라인 계정(예: 뱅킹), 영향을 받는 컴퓨터, 네트워크에 의존하는 기타 서비스가 포함될 수 있습니다. DoS 상태는 공격 대상이 응답할 수 없거나 단순히 충돌할 때까지 대상 호스트 또는 네트워크에 트래픽을 폭주시켜 정상적인 사용자의 액세스를 차단하는 방식으로 이루어집니다. DoS 사고는 악의적이지 않은 이유(예: 대량의 정상적인 인터넷 트래픽으로 인해 웹사이트가 중단되는 경우) 또는 사이버 위협 행위자의 행동으로 인해 발생할 수 있습니다.

과부하시키는 트래픽이 두 대 이상의 공격 컴퓨터로부터 동시에 발생하는 경우 DoS 사고는 분산 서비스 거부(DDoS) 공격으로 분류됩니다. DDoS 공격자는 봇넷(탈취되어 인터넷으로 연결된 장치 그룹)을 활용하여 대규모 공격을 수행하는 경우가 많은데, 이러한 공격은 공격 대상의 입장에서는 여러 공격자가 수행하는 것처럼 보입니다.

DoS 사고가 발생할 수 있는 시스템

공공 대면 서비스

- 유권자 또는 선거 정보 웹사이트
- 선거일 저녁 선거 결과 보도 웹사이트
- 온라인 서비스(예: 유권자 정보 조회, 투표소 조회, 유권자 등록, 우편/부재자 투표용지 신청, 후보자 등록 등)

인터넷 기반 사무 시스템

- 전자 선거인 명부
- 비즈니스 프로세스 시스템(HR, 회계, 전화 회선)
- 이메일 신청
- 인터넷 전화(VOIP) 시스템

악의적이지 않은 서비스 중단

선거 주기마다 전국의 관할 지역에서는 제한된 인터넷 대역폭, 잘못된 구성, 계획 또는 실행 미흡과 관련된 기타 사유로 인해 악의적이지 않은 서비스 중단이 발생합니다. 종종, 높은 온라인 트래픽 때문에 시스템이 과부하되어 일시적으로 사용할 수 없게 되는 경우가 있습니다. 또한 전화, 케이블, 광섬유 회선을 끊는 기상 이변이나 공사 사고 등 악의적이지 않은 사고로 인해 웹사이트 또는 시스템 중단이 발생할 수 있습니다. 이는 DDoS 공격인 것처럼 보이지만, DDoS 공격이 아니라는 점을 유의해야 합니다.

IT가 중요한 경우

선거 캘린더상의 중요한 날짜와 이벤트 시에는 선거 웹사이트와 온라인 서비스의 트래픽이 증가합니다. 관할 구역에서 제대로 준비되지 않은 경우 트래픽이 증가하면 서비스 중단이 발생할 수 있습니다.
유의해야 할 중요한 날짜와 이벤트:

- 전국 유권자 등록일
- 유권자 등록 추진, 캠페인, 마감일
- 우편/부재자 투표 신청 마감일
- 사전 현장 투표일
- 선거일 투표 시간 중
- 선거 결과 보도 중

DoS 사고에 대비하기

선거 관리 공무원과 선거 기술 제공업체에서는 DoS 사고의 가능성 및 영향을 줄이기 위한 사전 조치를 취할 수 있습니다.

서비스 제공업체와의 협력

잠재적인 DoS 사고 관련 위험을 완화하기 위한 핵심적인 첫 단계는 선거 관리 공무원이 사고 발생 전에 기존 계약을 검토하고 웹사이트 서비스 제공업체 및 인터넷 서비스 제공업체와 협력하는 것입니다. 이러한 협력을 통해 선거 관리 공무원은 사고가 발생하면 누구에게 연락해야 하는지 알 수 있으며, 서비스 제공업체에서 이미 시행 중인 보호 조치를 이해할 수 있습니다.

다음으로, 선거 관리 공무원은 추가적으로 어떤 DoS 완화 조치와 이중화 조치를 사용할 수 있는지 파악해야 합니다. 주요 서비스 제공업체에서는 대부분 기본 서비스는 무료로, 고급 서비스는 추가 비용을 지급하고 보호 기능을 이용할 수 있습니다. 사이버보안 및 인프라 보안국(CISA) 의 선거 보호용 사이버 보안 툴킷 및 리소스에는 선거 관리 공무원이 DoS 사고로부터 보호하기 위해 사용할 수 있으며 사이버보안 및 인프라 보안국(CISA), 사이버보안 및 인프라 보안국(CISA)의 합동 사이버 방어 협력체(JCDC) 회원, 기타 사이버 보안 커뮤니티에서 제공하는 무료 도구, 서비스, 리소스 목록이 포함되어 있습니다.

마지막으로, 선거 관리 공무원은 웹사이트 서비스 제공업체, 인터넷 서비스 제공업체, DoS 방어 서비스 제공업체 등 모든 서비스 제공업체와 사전에 조율하여 중요한 선거 날짜 및 장소 정보를 공유하고, 주요 기간에 충분한 문제 해결이 가능하도록 요청하며, 선거 운영에 영향을 미칠 수 있는 모든 계획된 유지 관리에 대해 상호 인식하도록 확인해야 합니다.

사이트 및 활동 모니터링

DoS 사고를 가장 잘 감지하고 식별하는 방법은 네트워크 트래픽을 모니터링하고 분석하는 것입니다. 네트워크 트래픽은 방화벽 또는 침입 감지 시스템을 통해 모니터링할 수 있습니다. 비정상적인 트래픽 부하가 감지되면 관리자는 경고를 생성하고 특정 기준을 충족하는 트래픽 또는 삭제된 네트워크 패킷의 출처를 식별하는 규칙을 설정할 수도 있습니다.

선거 관리 공무원은 서비스 제공업체와 협력하여 업체에서 이미 모니터링하고 있는 활동과 웹사이트의 '정상' 트래픽이 어떤 모습인지 더 잘 이해해야 합니다. 서비스 제공업체와의 협력 외에도 선거 관리 공무원이 자체 시스템에서 직접 찾아볼 수 있는 특정 지표가 있으며, 이는 잠재적인 DoS 사고를 나타낼 수 있습니다. 앞서 설명한 것처럼 이례적이거나 예상치 못했거나 비정상적인 활동을 성공적으로 식별하는 능력은 각 시스템 또는 서비스에 대한 '정상' 기준선이 무엇인지 이해하는 데 달려 있습니다.

이 지표에는 다음이 포함될 수 있습니다.

- 이례적으로 느린 네트워크 성능(파일 열기 또는 웹사이트 액세스 속도가 느린 경우 등)
- 특정 웹사이트를 이용할 수 없음
- 웹사이트에 액세스할 수 없음
- 애플리케이션 성능 저하

- 예상 못한 높은 프로세서 및 메모리 사용률
- 비정상적으로 높은 네트워크 트래픽

DoS 사고에 대응할 준비를 하세요

사이버 운영을 포함한 성공적인 선거 운영을 위해서는 탄력적인 프로세스가 필수적입니다. 이는 DoS 사고에 대응하고 그 영향을 완화하는 것을 포함하는 조직의 사이버 사고 대응 및 커뮤니케이션 계획을 위한 리소스를 확보하고 이를 실행하는 것을 의미합니다.

문제점 파악하기

잠재적인 DoS 사고가 발생했다고 판단되면 선거 관리 공무원은 네트워크 관리자에게 연락하여 중단이 유지보수 때문인지, 사내 네트워크 문제 때문인지 확인해야 합니다. 네트워크 관리자도 네트워크 트래픽을 모니터링하여 사고를 확인하고, 원인을 파악하며, 방화벽 규칙을 적용하고, DoS 보호 서비스를 통해 트래픽 경로를 다시 지정하여 상황을 완화할 수 있습니다.

선거 관리자는 네트워크 관리자에게 연락한 후 웹사이트 서비스 제공업체에 연락하여 네트워크가 중단되었는지, 네트워크가 공격을 받아 웹사이트가 간접적인 피해를 입었는지 문의해야 할 수도 있습니다. 이 경우, 웹사이트 서비스 제공업체에서는 적절한 조치 과정에 대해 조언할 수 있습니다. 서비스 중단이 중요한 선거 기간에 발생하거나 복구하는 데 상당한 시간이 걸리는 경우, 선거 관리 공무원은 정상적인 서비스가 허용 가능한 수준으로 복구될 때까지 백업 또는 대체 옵션을 사용하는 비상 계획이나 운영 연속성 계획을 실행할 준비를 해야 합니다.

공격이 발생하는 경우 선거 관리 공무원은 네트워크에 존재하는 다른 호스트, 자산, 서비스를 잊어서는 안 됩니다. 공격자는 DDoS 공격을 수행하여 노리는 표적으로부터 주의를 돌리고 네트워크 내의 다른 서비스에 대한 2차 공격을 수행할 기회를 노릴 수 있습니다.

사이버보안 및 인프라 보안국(CISA) 에서는 사이버 공격이 의심되는 경우 선거 관리 공무원과 선거 기술 제공업체에서 즉시 신고할 것을 권장합니다.

- 사이버보안 및 인프라 보안국(CISA), report@cisa.gov 또는 (888) 282-0870
- 미 연방수사국(FBI), 해당 지역 미 연방수사국(FBI) 현장 사무소를 통해
- 선거 인프라 정보 공유 및 분석 센터(EI-ISAC), SOC@cisecurity.org 또는 866-787-4722
- 관할권과 관련된 기타 주 당국 또는 지역 당국

정보 공유를 위한 대체 방법 준비하기

성공적인 선거 운영의 핵심은 회복탄력성입니다. 이는 DoS 사고 완화를 위한 비상 계획 또는 운영 연속성 계획을 수립하고 실행해야 함을 의미합니다.

DoS 공격을 받고 있는 선거 관리 사무소에서는 일반 대중, 다른 선거 관리 사무소, 심지어 같은 건물에 있는 다른 선거 관리 사무소와의 통신이 차단될 수 있습니다. 선거 관리 공무원은 각 선거가 시작되기 훨씬 전에 DoS 사고로 웹사이트나 기타 애플리케이션을 사용할 수 없게 될 경우에 대비하여 비공식 선거 결과 등의 선거 정보를 배포할 대체 방법을 마련해야 합니다. 이는 여러 방법으로 달성할 수 있습니다. 주 관할권 또는 지역 관할권에서는 기본 웹사이트와 완전히 분리된 인프라에서 백업 웹사이트를 호스팅할 수 있으며, 이는 유지보수 또는 업그레이드 기간 동안에도 사무실에 도움이 될 수 있습니다. 선거일 저녁에 보도 웹사이트를 운영하는 선거 관리 사무소에서는 주 네트워크 또는 지역 네트워크의 메인 웹사이트 및 다른 웹사이트에 결과 PDF를 업로드하는 것을 고려할 수도 있습니다. 마지막으로, 선거 관리 사무소에서는 사고 발생 시 정확한 투표소 정보, 비공식 선거 결과 등의 정보를 전달하는 데 도움이 될 수 있는 언론 매체와 관계를 구축하는 것을 권장합니다.

DoS 사고에 대한 내부 커뮤니케이션 계획 수립하기

선거 관리 공무원은 사고 대응 계획과 병행하여 DDoS 공격과 비악의적인 서비스 중단을 모두 커뮤니케이션 계획에 포함해야 합니다. 커뮤니케이션 계획에서는 위기 커뮤니케이션 팀(IT 및 커뮤니케이션 팀원 포함)을 식별하고, 역할과 책임을 정의하며, 사고 발생 시 커뮤니케이션 채널을 유지하기 위한 절차를 수립해야 합니다. 위기 커뮤니케이션 팀에서는 기본 사무실 네트워크나 휴대폰에 액세스하지 않고도 커뮤니케이션을 유지할 수 있도록 준비해야 합니다. 선거 관리 공무원은 모든 직원이 사용하도록 DoS 사고 관련 주요 용어 및 정의 목록을 개발하는 것을 고려할 수도 있습니다.

선거 관리 공무원은 DoS 공격 발생 시 필요에 따라 수정하여 사용할 수 있는 보유 성명서를 준비하는 것도 고려해야 합니다. 보유 성명서는 고위 직원 및 커뮤니케이션 담당자뿐만 아니라 일반 대중과 언론의 전화에 응답하고 질문을 받는 일선 직원에게도 제공되어야 합니다.

DoS 사고 대비 계획 및 교육

앞서 설명한 바와 같이 선거 관리 공무원은 비상 상황, 운영 연속성, 사고 대응, 복구 계획에 DoS 사고 시나리오를 포함해야 합니다. 이러한 계획에는 조직에서 이러한 사고를 식별하고 완화하며 신속하게 복구하고 사고 대응 및 복구 전반에 걸쳐 효과적인 커뮤니케이션을 유지하도록 안내하는 내용이 포함되어야 합니다. 사이버보안 및 인프라 보안국(CISA) 의 선거 보안을 위한 사이버 사고 감지 및 알림 계획 가이드(Cyber Incident Detection and Notification Planning Guide for Election Security)는 조직에서 사고 대응 계획을 수립하는 데 도움이 될 수 있습니다.

다른 사이버 사고와 마찬가지로 DoS 사고 대응 계획에는 조직 리더, 서비스 제공업체 등 모든 이해관계자의 역할과 책임이 명확하게 규정되어 있어야 합니다. 해당 계획에는 최소한 사고 확인, 사고의 성격 파악, 완화 조치 배포, 효과 모니터링, 복구에 대한 절차가 개략적으로 나와 있어야 합니다.

특히 내부 커뮤니케이션 채널이 중단으로 인해 영향을 받는 경우(예: 인터넷 전화 시스템에 액세스할 수 없는 경우) DoS 사고에 대한 계획에는 운영의 연속성 및 재해 복구 절차도 고려되어야 합니다. 조직의 리더십은 직원, 서비스 제공업체, 유권자에게 신속하고 효과적으로 연락할 수 있는 백업 또는 대체 커뮤니케이션 채널(예: 전화 연락망, 대체 이메일, 긴급 알림 시스템)을 숙지하고 있어야 합니다.

사고 후 서비스가 복구되면 선거 관리 공무원은 사고 브리핑을 실시하여 사고 대응 및 커뮤니케이션 계획 실행을 통해 얻은 교훈을 논의하고 그에 따라 절차를 업데이트해야 합니다.

마지막으로 모든 직원은 사고 대응 교육을 받고 정기적으로 연습을 실시해야 합니다. 선거 관리 공무원은 모의 훈련 또는 기타 시나리오 기반 훈련에 DoS 사고를 포함하는 것을 고려할 수 있습니다. 정례적인 연습은 모든 개인이 사고 발생 시 자신의 역할과 책임을 이해하고, 대응 계획의 미흡한 부분을 파악하며, 이해관계자가 실제 사고의 긴급성과 흐름을 연습하고, 계획과 완화 조치 모두에 대한 신뢰를 구축하는 데 있어서 아주 중요합니다. 사이버보안 및 인프라 보안국(CISA) 의 선거 사이버 대응 모의 훈련(Elections Cyber Tabletop in a Box) 리소스에는 연습 시나리오의 일환으로 DDoS 공격이 포함되어 있습니다. 사이버보안 및 인프라 보안국(CISA) 의 지역 사이버 보안 고문(CSA)은 DoS 사고에 대한 위험 관리 지침을 포함한 평가 및 보호 리소스도 제공합니다.

추가 리소스

이 가이드에서 제공하는 정보는 문서 전체 및 아래에 링크된 추가 리소스를 통해 보완됩니다. 선거 관리 공무원과 선거 기술 제공업체에서는 이러한 리소스를 검토하여 잠재적인 DoS 사고와 관련된 위험에 더욱 잘 대비하고 완화할 것을 권장합니다.

- CISA FBI MS-ISAC 분산 서비스 거부 공격에 대한 이해와 대응
- CISA 분산 서비스 거부 공격에 대한 이해
- CISA 선거 보호를 위한 사이버 보안 툴킷 및 리소스
- CISA 분산 서비스 거부(DDoS) 빠른 가이드
- CISA 선거 보안을 위한 사이버 사고 감지 및 알림 계획 가이드
- CISA 선거 사이버 테이블 탑 인 더 박스
- CISA 역량 강화 가이드: 웹 서비스에 대한 볼류메트릭 DDoS 기술 가이드