Website Security

An election office's website is often the first and most important source of information for voters, the media, and other interested parties. It is extremely important to have a secure website that is resistant to attacks and provides critical information with an official, professional manner and appearance.

Introduction

This best practice covers five important topics about websites, as detailed below.

The .gov top-level domain

Top-level domains are important to understand both from a cybersecurity perspective and to know how constituents will engage with and access your web presence. The ".gov" domain suffix is restricted to verified U.S. government entities, which helps ensure legitimacy for visitors browsing U.S. government websites. Additionally, ".gov" domain owners are required to maintain a higher level of security, and the federal government has implemented several cybersecurity controls in the underlying infrastructure.

As .gov domains are carefully controlled, once you have one you can communicate to your constituents that they should only trust a .gov for official information.

Securing a site with HTTPS

Hyper Text Transfer Protocol Secure (HTTPS) is an internet communication protocol used to encrypt and securely transmit information between a user's web browser and the website they are connected to. HTTPS accomplishes this through the use of a Secure Sockets Layer (SSL) certificate, which establishes an encrypted connection. The certificate also helps authenticate that the website and the user are who they say they are when communicating.

HTTPS is the norm across the internet. Major web browsers label websites that do not use HTTPS as "not secure" and often require users to take additional steps to visit the site. Even if the site doesn't contain malicious content, this can dissuade people from trusting your official site.

Denial of service attacks

A denial of service attack (DoS) seeks to disrupt the availability of a system or service. Additionally, threat actors may use multiple source computers in a distributed denial of service (DDoS) attack.

Typically, these attacks target webservers in order to overwhelm the webserver's internet connection or its ability to respond to user requests. If the threat actors can send more requests than permitted by the system, the webserver or internet connection will be too busy to respond to additional requests, resulting in a "denial of service" to legitimate users. Of note, computers participating in a DDoS attack may be infected with malware that conducts the attack, which means they are also victims of malicious activity.

Typosquatting

Typosquatting attempts to take advantage of errors users might make when URLs are typed directly into the address bar. Similarly, malicious actors may seek to trick users into taking a quick glance at a URL and opening a visually similar yet malicious link.

Website defacements

Website defacements are the unauthorized modification of web pages, including the addition, removal, or alteration of existing content. Websites that are unpatched or misconfigured are easily susceptible to simple probing tools used by these actors, which can lead to unauthorized access to websites.

While in most cases they seem to be simply a nuisance, website defacements pose a potential public relations concern for election offices and could promote disinformation, including the alteration of time and dates for open voting events or unofficial results. These changes may be subtle and thus difficult to detect.

Goals

1. Move your website to the .gov top-level domain (Level 1 maturity)
2. Use HTTPS everywhere (Level 1 maturity)
3. Prevent denial of service attacks (Level 1 maturity)
4. Understand typosquatting and what to do about it (Level 1 maturity)
5. Know about website defacements and how to prevent them (Level 1 maturity)
6. Enroll in the EI-ISAC's vulnerability disclosure program (Level 2 maturity)

Actions

For Website Security, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

1. Visit https://get.gov to sign up for and manage a .gov website and email domain.
   - Effectively managing a website can be difficult, but the good news is that you can mitigate many of the risks with one simple step: getting a .gov domain. A .gov domain automatically provides HTTPS and reduces the likelihood of your constituents confusing other websites for yours.
2. Stop denial-of-service (DOS) attacks by using no-cost tools.
   - Tools, including those from from Cloudflare and Google, will mitigate instances of these attacks.
   - Learn more through the EI-ISAC's Guide to DDoS Attacks.
3. Reduce the risk of typosquatting by:
   - Communicating that your .gov site is the only official site.
   - Register or purchase variations of your domain, such as your domain but with .com, .org, and .net addresses and common typos that might occur.
4. Manage website defacements by:
   - Developing a plan to defend against and recover from website defacements.
     - Consider temporarily pulling down the site to prevent any further misrepresentation.
     - Have a recovery plan created on how to alert readers about the targeted website.
     - Have offline backups established that can be quickly deployed in place of a compromised website.
   - Maintain up-to-date software and patch vulnerabilities.
   - Enroll in CISA's CyHy program or the EI-ISAC's Vulnerability Assessment to receive notifications on outdated software.

Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Establish a vulnerability management program (VDP): A VDP is a formalized process to receive, validate, remediate, and communicate vulnerability information identified by security researchers on specific technology systems.
   - By working with external security researchers, organizations can broaden their vulnerability management efforts and remake them as a continuous process—all while saving time and money.
   - The EI-ISAC offers a VDP that makes it easier for election offices to create and operate a VDP. Contact elections-vdp@cisecurity.org for more information.

Cost-Effective Tools

- get.gov: The government portal to obtain and manage a .gov domain.
- CyHy program: CISA's cyber hygiene web application scanning program.
- Cloudflare's Athenian Project: Free security and performance for state and local election websites.
- Google's Project Shield: A free service that defends news, human rights and election monitoring sites from DDoS attacks.

Learn More

- Election Security Spotlight – Typosquatting
- The distributed denial-of-service (DDOS) attack section of CISA's Cybersecurity Toolkit to Protect Elections.
- CISA's DDOS Quick Guide.

Mapping to CIS Controls and Safeguards

- There are no relevant CIS Controls

Mapping to CIS Handbook Best Practices

- 9