CENTER FOR
DEMOCRACY
& TECHNOLOGY

ELECTIONS
Short, simple, usable guides to help election administrators and staff better understand key concepts in cybersecurity.

CLOUD

Election Cybersecurity 101 Field Guide: Cloud Services

[What Are Cloud Services?]

Cloud services are software-based services delivered via the internet, rather than maintained and managed on-site. They allow organizations, like election agencies, to contract external companies to manage necessary tasks like hosting a website or managing a database.

[Why Are Election Entities Using Cloud Services?]

Election-related organizations like election administrators and political campaigns have to maintain a number of online services, such as voter portals (where citizens can register to vote and find information like polling places), voter registration databases, voter mailing lists and engagement services, and websites for their campaign or agency. Maintaining and securing the systems and physical hardware required to provide these services can be expensive for election agencies, and requires substantial expertise to ensure that voters and elections are protected. Oftentimes, it may be prohibitively expensive for these agencies to acquire the level of expertise they would need (particularly since building out these services may take a wide variety of expertises, which would either translate to multiple employees, or one employee with difficult-to-find skills). Providers of cloud services typically have this expertise internally, and are able to provide it more cheaply to election customers.

[What Are the Concerns or Pitfalls?]

One of the key concerns with cloud services is ensuring that they are correctly configured for the high security and privacy needs of the election context. While ideally these cloud services would default to secure configurations, many of them were not designed with an election context in mind and consequently their default settings are not sufficiently secure. Incorrectly configured services can lead to security concerns like exposed voter data or tampered websites, or usability concerns like inaccessible websites. Thus, election agencies will still need to ensure that they have some internal expertise: they will still need someone familiar with using the cloud service selected, even if they are not an expert in each of the things the service provides.

[Securing Cloud Configurations]

The main component of securing a cloud service is ensuring that access is restricted only to those that need it. There are a number of considerations: The first are standard access control mechanisms, like individual accounts with strong passwords. Although shared organizational accounts are sometimes necessary, they do require extra governance to ensure they are secure. For example, if a staff member who had access to a shared account leaves, the password to that account must be updated. Additionally, individual accounts should have the minimum permissions necessary to do the work. For example, if a staff member is responsible for reading raw data and organizing it into a report, that person should have permission to read the data, but not to update or delete it.

In addition to appropriate access control, organizations using cloud services should take a “defense in depth” approach, and have plans in place in the event that primary security mechanisms fail. For example, ensuring that data is encrypted at rest (meaning that data is encrypted before it is stored, so even if it is breached, the data will be unreadable to the attackers) means that the impact of a data breach can be mitigated. Organizations should also have a response plan in place, to ensure there are clear and comprehensive steps outlined in response to an issue like a data breach or data leak.

[IMPORTANT]

- ➢ **The Cloud is Real:** Something in “the cloud” ultimately exists in a physical place somewhere. The cloud service can provide access to the information on the server anywhere with internet access, but the jurisdiction of that server’s location may be important when deciding on a cloud provider, as information stored in foriegn jurisdictions would be subject to those laws and potentially accessible to government actors in those countries.

- ➢ **Cloud Services are Vendor Subcontracts:** A key part of employing a cloud service is setting expectations around what the service will provide, what guarantees it will make about those services, and what happens if those guarantees are not met. These factors are typically laid out in a Service Level Agreement (SLA) contract. The SLA typically incorporates what the provider will be responsible for and what the customer will be responsible for (i.e. the provider may offer hosting and backup for a database, but not offer any validation of input data, so the customer would be responsible for validating data before inputting it into the database), what guarantees the provider makes (like guaranteeing that the customer’s website will be available at least 99.99% of the time over the course of a year), and what will happen if the contract is breached (i.e. if the website is down more than 99.99%, the customer does not have to pay the provider).

- ➢ **Data Loss is a Risk:** In addition to availability, cloud services should also be able to tell you about data redundancy, or backups. Most cloud services replicate the data they store in more than one place to ensure that the data will still be available if one copy of the data is lost. Your cloud provider should be able to tell you about how they ensure the availability of data, and how quickly they can recover if access to one copy is lost. Additionally, this is another place to consider jurisdictional concerns. Many cloud services have data centers in geographically diverse locations to minimize the impact of things like natural disasters. If you have requirements about where data can be stored, check with your provider to make sure they can meet these requirements while still offering sufficient data redundancy.

[Additional Resources]

- Procuring technology for elections: https://www.cisecurity.org/elections-resources/
- Building a data breach response plan: https://www.comptia.org/content/guides/data-breach-response-plan
- The FedRamp program: https://www.fedramp.gov/
- Further discussion of risks in the cloud environment, as well as additional resources: https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

For more info, contact Mallory Knodel: mknodel@cdt.org. Other election security resources: bit.ly/CDTelectsec.