How to Protect Voting Machines and Voter Registration Data From Hackers

There has been a lot of news about the voting machines and the voter registration databases being hacked in precincts across the United States. Here is a simple step to protect both: Do not let the computers be connected to the Internet.

This is straightforward protection, since almost all the hacking has been done over the Internet. It is not necessary for our voting machine computers nor our voter registration computers to be connected to the Internet. For example, our voting machines do not need to support email. They just need to support secure voting.

So here's a simple model used by information security practitioners to provide easy to understand security.

1. Keep the computers in a locked room. When it's time to vote, put the voting machines in the room where the voting takes place, but keep them monitored so that no one can touch the computers themselves without being seen.

2. Don't connect those computers to the Internet. Don't connect them to other computers that are connected to the Internet.

3. You may connect those computers to each other in a local network (LAN or Local Area Network) without connecting to the Internet. Ask your information security practitioners to make your LAN reasonably secure.

4. When some trusted person needs to update the software on the computers, or to download the data on them, give that person the key to the locked room. Let her use USB or similar storage devices to perform updates and downloads. Have her return the USB device along with the key to you when she is done.

5. Take backup copies of the data and store them in a secure location.

6. Note that you can use USB storage devices that automatically encrypt the data both for updates and downloads and for backups of data.

7. When it's time to report election results, have a trusted person in each precinct call the results in to your central location, using a password or a secure phone to prove who he is. Later you can use USB devices to carry all the data to the central location without using the Internet.

How to Protect Voting Machines and Voter Registration Data From Hackers

These simple steps will take you a long way towards securing our elections, without a lot of expense or effort. You can ask any auditor you know to volunteer a little time to review your operation and make suggestions to protect your data even better.

It is much easier for a hacker in some foreign country to hack a lot of voting machines in a short time if they are connected to the Internet. If on the other hand, the only way to access them is by being in the room with the computer, then it would take an army to hack every precinct in the United States.

I hope you will share this suggestion with the people who run the elections in your precinct. I welcome your comments and suggestions on this at stu@stuhenderson.com . Thanks.

PS If you'd like to learn about how bots (computer programs pretending to be humans posting on FaceBook and other sites) influence public opinion and elections, please see http://www.ndn.org/sites/default/files/blog_files/NDN-BOTPAPER.pdf.

About the Author:

Stu Henderson is an information security auditor, consultant, and trainer. He likes to share with others what he has learned.