Securing Democracy: The Role of Ethical Hacking in Election Security

Ruijgrok T, Tiemen

10/10/2023

Table of contents

1. Summary

This research delves into the critical topic of election security, focusing on the role of ethical hacking in safeguarding digital elections. It explores vulnerabilities in election systems, potential consequences of hacking, and technological advancements for enhanced security. Ethical hackers, experts who protect digital systems legally, play a vital role. The study emphasizes the importance of ethical hacking but acknowledges it is not a complete solution due to evolving threats. It provides practical recommendations, such as investing in skilled ethical hacking teams, user training, and robust cybersecurity measures. While challenges persist, ethical hacking coupled with proactive cybersecurity efforts stand as essential tools against election tampering, ensuring the integrity of democratic processes worldwide.

2. Introduction

In today's world, where technology plays a big role in our lives, the security of our elections is incredibly important. Elections are when we choose our leaders, and they must be fair and honest. However, there are times when people with bad intentions try to break into the computer systems we use for elections, which can cause significant problems.

Subject Description

This research focuses on how a special kind of computer expert, known as an ethical hacker, can help improve the security of our elections. Ethical hackers are like the good guys in the digital world. They look for weaknesses in computer systems, but they do it to protect our elections and not to cause harm.

Social Importance

The reason we are studying this is because elections are a cornerstone of our society. They are how we make important decisions about our government and our future. If someone interferes with our elections, it can make people lose trust in the entire system, which is not good for our democracy.

Question

The main question we aim to answer is: "How can ethical hacking contribute to the enhancement of election security and the protection of election processes in the digital age?"
To address this question, we will explore three smaller questions:

- What are the key vulnerabilities in election systems? This will help us understand the challenges that ethical hackers face.
- What are the potential consequences of election hacking? This will show us why it is crucial to prevent such incidents.
- How can technology advancements enhance election security. We will explore if there are ways to make elections safer.

Objective

This research aims to demonstrate how ethical hacking can contribute to the security of our elections. By researching the problems, consequences, and recent technology, we could find ways to ensure the integrity of our democracy.

Definition

In this research, "ethical hacking" refers to the work of computer experts who function as digital protectors. They use their skills to find and fix problems in election computer systems with permission to ensure our elections remain fair and trustworthy.

3. Methodology

This study's plan was designed to understand election security, focusing on ethical hacking and tech solutions. Methods were selected based on thorough analysis of past research and real-world cases.

Description of Research Population

The study included a range of individuals, such as cybersecurity experts and global participants in the electoral process. This was important to gather different opinions and make sure the study's findings were globally relevant.

Description of Data Collection

Analysis was performed on cybersecurity reports and vulnerability cases, providing qualitative and quantitative data crucial for a good understanding of the subject matter.

Analysis Proposal

The study used a variety of methods to look at election systems. Numbers were studied to find problems and trends. Words from interviews were studied to understand ethical hacking better. Articles were consulted from studies on election security that have already been extensively conducted.

4. Threads of Election Security

There is this article “Hacking the vote: It’s Easier Than You Think” about Alex Halderman who has made a career studying electronic voting security. This article shows how easy it was to hack the voting machines in the U.S.

“After the 2000 election debacle in Florida, with all those hanging chads and confusion about voter intent on paper ballots, Congress gave states more than $3 billion to modernize their voting machinery. As a result, there was a widespread shift toward using touchscreen voting systems and computerized tabulations. However, very few states or equipment vendors allowed independent researchers to examine the security of these machines. So, in 2006, Felten (Halderman’s, graduate student at the time, mentor) contacted an elections insider willing to slip him a commonly used model.” Through this voting machine, they made a YouTube video showing the machine being hacked in a mock election in which Benedict Arnold wins the presidency despite voters clearly choosing George Washington.

In 2010, the District of Columbia was planning to allow citizens to vote via the internet in municipal elections. “Online voting is, to Halderman, a particularly terrible idea and one that he has worked against by exposing security flaws in systems used in Australia, Estonia, and Norway.” Halderman speaks the truth here because online voting is incredibly vulnerable. They should only stick to well secured counting systems to minimize the exposure to the (potentially bad) people. The result of not doing this was hackers who easily broke into the systems, altering votes without detection. So after this, district officials canceled the online voting idea and never returned to it.

“The only way to know whether a cyberattack changed the result is to closely examine the available physical evidence — paper ballots and voting equipment in critical states like Wisconsin, Michigan, and Pennsylvania,” Halderman wrote. That is why for instance The Netherlands uses only paper ballots for all elections. After you filled in your ballot, you must throw it into a physically secured container. This way they minimalize the risk of changed results by cyberattacks in the voting round. Now the only digital vulnerability in the countries that use this voting system is the counting software.

Vulnerability example in Election Vote Counting Software

Another article with an example of a vulnerability in an election system: “Hacker Discovers Vulnerability in Dutch Election Vote Counting Software: Less Than an Hour's Work.” A vulnerability in the vote counting software used in Dutch elections potentially allowed manipulation of election results. Although there is no evidence that manipulation occurred, a hacker who discovered the vulnerability reported it to the Dutch Electoral Council (Kiesraad), and the issue has since been resolved. The vulnerability could have enabled malicious actors to access the infrastructure of the software provider responsible for the vote counting software. This access could have allowed the distribution of a modified, manipulated version of the software, potentially altering election outcomes.

The software provider detected "a number of login attempts," according to the Kiesraad. However, there is no indication that these attempts led to misuse of the software. Additionally, post-vote sampling is conducted to verify the accuracy of the counts, making it likely that any fraudulent activity would have been detected.

The hacker who identified the issue found that login credentials of the software provider were present in the installation software. This allowed access to the provider's infrastructure, including the part housing the vote counting software. The hacker could have introduced a customized version of the software. Whether this alone would have been sufficient to manipulate elections is uncertain, as municipalities are supposed to verify the digital signature of the software before using it.

The hacker, Maarten Boone, claims to have spent less than an hour identifying the vulnerability and commended the swift response and resolution by the Kiesraad's head of IT security. He also expressed satisfaction with the practice in the Netherlands, where hackers with good intentions can report vulnerabilities in computer programs safely and without fear of prosecution.

The reason that the vulnerability was in the installation software was because security tests did not examine the installation software. To prevent further hacks in this area, the installation software is now included in security tests. In this example, there is no mention of an ethical hacker (white hat hacker), but rather a grey hat hacker (someone who is engaging in hacking activities without explicit authorization but may have good intentions, such as identifying and disclosing security weaknesses to organizations or the public). Fortunately this is not the case, because it could have turned out very differently if a hacker with malicious intentions (black hat hacker) had leaked or taken advantage of this vulnerability.

5. The role of ethical hackers

Experienced ethical hackers are crucial for finding system weaknesses. It is better to invest in a skilled team rather than a cheap one that might miss important vulnerabilities. This applies to all significant systems, not just to elections. Spending a bit more on a good team is wise. It is more cost-effective in the end, preventing potential breaches and data leaks compared to the higher costs resulting from a cheap team missing critical security issues. In the summer of 2020, ethical hackers examining Colorado's voter registration website found a critical issue related to the site's CAPTCHA challenge, a common online security measure. According to an article by Statescoop, this flaw could have allowed a distributed denial of service (DDOS) attack or enabled further malicious activities, posing a serious threat during an already challenging election year. The ethical hackers identified bugs in the CAPTCHA implementation that previous testers had not noticed. This discovery highlighted the importance of having skilled ethical hackers working closely with state officials. Their expertise ensured a thorough evaluation of the system, emphasizing the necessity of comprehensive security measures to safeguard the election process.

Crowdsourced Security vs. Vulnerability Disclosure Programs

In cybersecurity, there are two main approaches besides hiring a hacking team or company: Vulnerability Disclosure Programs and Crowdsourced Security Testing Platforms. Vulnerability Disclosure Programs encourage people to report security flaws they find. On the other hand, Crowdsourced Security Testing Platforms go a step further. They involve ethical hackers from around the world actively testing digital systems, getting paid for finding vulnerabilities. These platforms offer a mix of skills, encourage healthy competition, provide continuous testing, and are cost-effective. Their competitive environment and large pool of experts make them a powerful tool for organizations to find and fix security issues, making them a top choice for enhancing cybersecurity.

Apart from the mentioned methods of securing elections, employing a skilled ethical hacking team is superior to relying on random hackers globally. Allowing just anyone access to such a system worldwide is not ideal and could pose significant risks.

Voter Registration Database Security (2022)

The system software that counts the votes and the underlying systems is a major digital factor that can be hacked. The center for election innovation and research (CEIR) made a report about the Voter Registration Database Security (VRDB) in 2022. Every two years, CEIR carries out a survey to evaluate the security status of VRDB (Voter Registration Database) in the United States. This survey focuses on three key aspects: preventing security breaches, detecting potential threats, and mitigating risks. The results from both the 2018 and 2020 surveys highlighted how seriously states view cybersecurity concerns, underlining their dedication to addressing these issues.

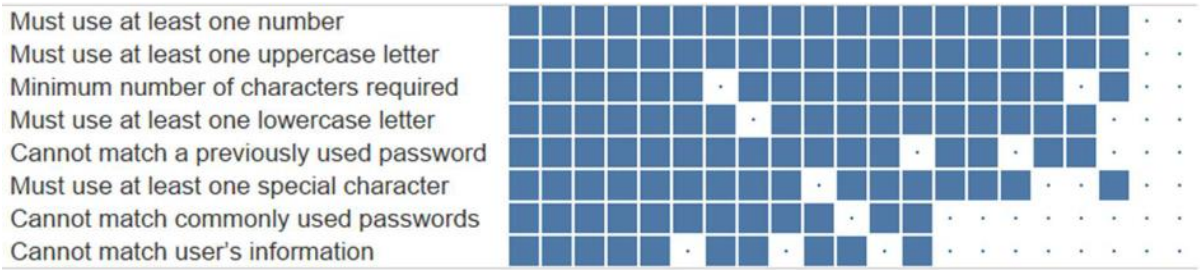
Prevention

The first step in making sure a computer system is secure is to find and fix any weaknesses. To protect VRDBs and the sensitive information they hold, administrators control who can access them, monitor the system to keep it secure, teach people how to recognize and deal with online threats, and set up rules for email security. So, we use both technology and education to prevent problems. The following chapters describes some aspects of securing a VRDB and the precautions to take.

User access – passwords

Cybersecurity experts recommend complex passwords or frequent changes, if not they can lead to insecure practices. The National Institute of Standards and Technology (NIST) suggests passwords be at least eight characters long. Some states still require special characters in passwords, but the number of states requiring a minimum character length has slightly decreased. The trend may reverse, with more states adopting minimum length requirements in the future, following NIST guidelines.

Figure 1: Password Requirements: States that Responded in 2022



Multi-Factor Authentication

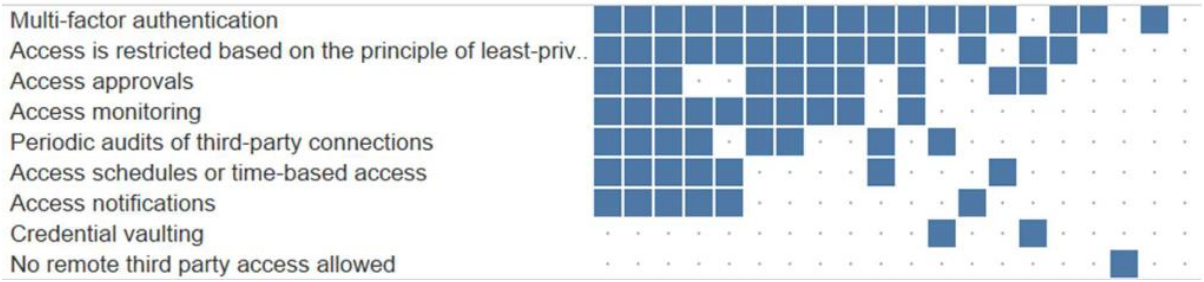
Multi-factor authentication (MFA) enhances VRDB security by requiring users to provide a second authentication factor, in addition to a password, when accessing the system. This extra layer helps protect against threats like phishing. In recent years, there has been an increase in the adoption of MFA among states, with twenty out of twenty-two states requiring it in 2022. The most common types of MFA used include physical devices, time-based one-time passwords (TOTP), and SMS authentication. This trend shows substantial growth from 2018 to 2020 and moderate growth from 2020 to 2022 in the use of MFA.

Figure 2: Multi-Factor Authentication Requirement: States that Responded in 2020 and 2022

Third-Party Access

States sometimes need to grant third parties access to their VRDB systems, even for critical security processes. To manage the associated risks, states employ various security measures. In 2022, CEIR's VRDB security survey found that many states use Multi-Factor Authentication (MFA) for third-party access, restrict access to the principle of least privilege, monitor access, practice access approvals, conduct periodic audits of third-party connections, and employ time-based access.

Figure 3: Practices for Securing Remote Third-Party Access: States that Responded in 2022



System Integrity – Audits

Apart from just making sure the right people can access VRDB systems, states also need to keep these systems safe from cyberattacks and working smoothly all the time. To achieve this, VRDBs and related systems should be built in a way that considers the limitations of users when it comes to security. While there is not a single solution that guarantees system integrity, using different security methods, having skilled IT staff, and regularly taking care of the system can make VRDBs stronger against outside attacks. All systems that connect to the internet, including VRDBs, should be regularly audited to ensure security and functionality. This involves good IT support from experienced IT staff.

User Training

In the same way that a system should be set up to reduce the chances of human mistakes, users need training to minimize vulnerabilities. Even if a system is incredibly secure, it can still be at risk if a user shares their login information or does something unsecure. Therefore, VRDB users should be taught how to recognize and deal with cyber threats they might come across.

Figure 4: Cyber Threat Training Frequency: States that Responded in 2022

Phishing, a technique that can trick the most careful users into giving their login details, remains a big issue in cybersecurity. To reduce this, according to CEIR users also get trained to counter the risk of getting phished.

Tabletop Exercises

States frequently use tabletop exercises (TTXs) to train election administrators. These exercises create scenarios that imitate the most challenging situations that might happen during an election. Participants then talk about the right steps to take in different situations and practice responding quickly to various crises.

Email Security Protocols

Email protections are crucial for preventing phishing attacks and blocking harmful email attachments that could compromise a VRDB. These protections typically verify the sender's authenticity or check the contents of emails.

Figure 5: Email Protections: States that Responded in 2022

Detection and monitoring- Login Attempts

Keeping an eye on and reviewing attempts to log into a VRDB, whether those attempts are successful or not, is a crucial step to identify potentially harmful actions. Apart from trying to break in through login attempts, malicious actors might also try to harm VRDBs by inserting commands or code into the database to change the system or gain control over the backend.

Traffic

States also keep an eye on how VRDB activity changes over time. They need to be aware when VRDB activity does not follow its usual patterns, so they can figure out why this is happening. Sometimes, more VRDB activity is harmless, like when there is a big voter registration drive. But sometimes, it could be because of bad actors. Also, if important records, like those of celebrities, get changed, it could be a sign that someone is messing with the VRDB.

Network Monitoring Systems

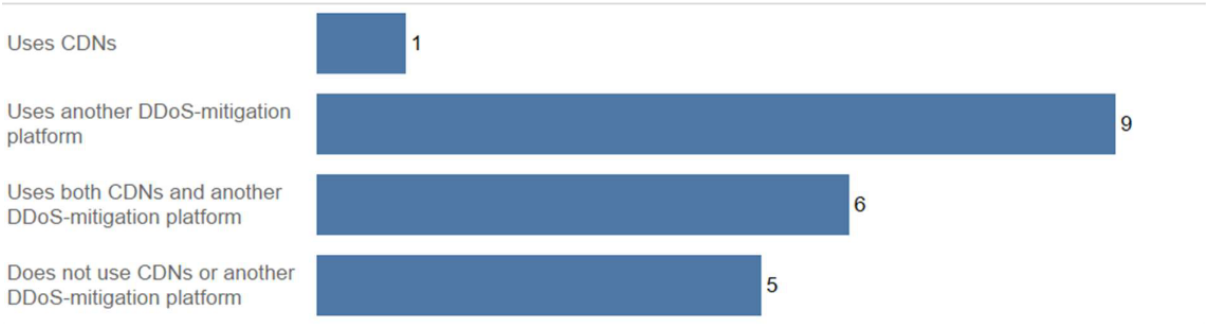
Network monitoring systems are frequently employed to identify potential risks to a VRDB. These systems continuously keep an eye on external network traffic to actively prevent unauthorized access to the VRDB or notify IT personnel if something suspicious is detected. An efficient way of doing this is by pairing an intrusion detection system with real-time expert threat analysis.

Mitigation - CDNs and DDoS tools

When a cyberattack is detected, states need to respond quickly. They can use resources like content delivery networks (CDNs) and distributed denial-of-service (DDoS) mitigation tools to make sure the VRDB remains accessible to authorized users, even during an attack. Additionally, practices such as regular system backups and the use of paper pollbooks are part of contingency plans to restore systems and reduce the impact of a successful attack on the VRDB.

DDoS attacks are a common method used by malicious actors to disrupt legitimate user's access to a website or networked system by consuming all available resources. CDNs and also DDoS mitigation tools are effective ways to keep networked systems functioning and available during such attacks.

Figure 6: CDNs and DDoS-Mitigation Platforms: States that Responded in 2022



Backups and Pollbooks

When all else fails and an attack manages to change or disrupt a VRDB, there should be a plan in place to both fix the system and make sure elections can still happen as they should. Contingency plans, including backups and pollbooks, are crucial to prevent major disruptions to the election process.

Regularly backing up the VRDB is the best way to ensure voter data is not permanently lost. States have different policies on how long they keep these backups, ranging from one week to indefinitely, with most preserving them for at least a year.

In case of an attack on Election Day, states can rely on pollbook backups and provisional ballots. The specific methods used depend on the types of pollbooks each state uses, and sometimes states use multiple types for a single election.

All precautions mentioned apply not only to the U.S. states, but also to all VRDBs that exist around the world for every country using this system. There are always more precautions that can be taken, these are just the most important measures where things go wrong most often.

Other methods to enhance election security

In addition to making election systems secure by ethical hackers, more measures that have not yet been mentioned can be taken to reduce the need for ethical hackers.

Software and Patch Management

Implementing a comprehensive software and patch management program is crucial for an organization's cybersecurity. Such a program involves creating a detailed list of all software in use, enabling the organization to understand potential vulnerabilities. This knowledge allows them to identify and reduce risks in their IT infrastructure, particularly in election-related systems. The absence of a patch management program often leads to network compromises due to common, readily available malware. Such breaches could result in severe consequences like ransomware attacks or data theft. Timely deployment of patches is vital to avoid becoming an easy target for cybercriminals. If a full patch management solution is costly, enabling automatic updates is a suitable alternative.

Network Segmentation

Organizations can effectively limit the impact of potential attacks by implementing network segmentation. Proper network segmentation prevents intruders from spreading their exploits or moving laterally within a network. A well-segmented network categorizes various parts based on their roles and functions, which prevents malicious intrusions from affecting critical devices or accessing sensitive data. In instances where network segmentation is lacking, intruders can gain control over crucial devices or acquire access to valuable data.

Disable SMB v1

To safeguard networks of organizations, they should take specific actions against a recent threat identified by CISA. Threat actors have been utilizing SMB v1 (Server Message Block version 1) to distribute malware within organizations. To counter this threat, CISA recommends disabling SMB v1 Internally: Organizations should internally disable SMB v1 on their network. This ensures that the vulnerable version of the protocol is not used within their systems. Also organizations should block SMB Traffic at the Network Boundary such as specific port numbers to prevent malware spread through SMB protocols.

Establish a Baseline for Host and Network Activity

An organization's IT staff play a crucial role in identifying normal and expected activities on hosts and networks. They can use specific metrics to establish these normal patterns. For network activities, these metrics include expected bandwidth usage for the organization, individual users, remote access, ports, protocols, file types, and even the timing of activities.

For individual hosts, organizations can establish baselines by creating a standard setup (known as a "gold image") for workstations and servers. This image includes trusted applications and configurations unique to the organization. Critical files' hashes, software for remote host access, approved software lists, and configurations allowing automatic software launches should be documented.

Notice and Consent Banners for Computer Systems

This outlines key elements for effective notice and consent banners in computing systems, emphasizing the need for clarity and user acknowledgment. These elements are essential in ensuring users understand the terms of monitoring and data handling. The banner should expressly cover data and communication monitoring, allowing disclosure to any entity, including government bodies, and should specify that monitoring can occur at any time and for any purpose.

6. Discussion

However, this study is not a complete solution. Ethical hacking helps, but it is not perfect, and cyber threats keep changing. The study mostly looks at the United States, so it might not apply everywhere.

Looking ahead, more research is needed to understand new threats worldwide. Different countries have different political systems and technologies, so we need to learn from each other.

7. Conclusion

In summary, this research dives deep into how ethical hackers play a crucial role in keeping our digital elections safe. It explores the vulnerabilities in election systems, the risks of hacking, and how technology can make elections more secure.

The research shows that ethical hacking is essential. It helps identify and fix vulnerabilities in election systems. The study highlights the urgent need for action because there are risks and vulnerabilities in these systems. Practical suggestions include investing in skilled ethical hacking teams and strong cybersecurity. Regular checks, user training, and using secure passwords are vital. Also, updating software, dividing networks, and blocking vulnerable methods can enhance security. Clear rules for users and transparent banners are important too.

In conclusion, while challenges remain, this research shows that ethical hacking and smart cybersecurity efforts offer hope against election tampering. By using these strategies and staying alert to new risks, countries can protect their elections, ensuring they are honest and trusted by everyone.

Source list

Alumni Association of the University of Michigan. (2021, 19 November). *Hacking the vote: It's easier than you think - Alumni Association of the University of Michigan*. https://alumni.umich.edu/michigan-alum/hacking-the-vote/

Best Practices for Securing Election Systems | CISA. (2022, 11 November). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/best-practices-securing-election-systems

Freed, B. (2021, 3 september). Colorado official details plans for penetration testing of election systems. *StateScoop*. https://statescoop.com/colorado-official-details-plans-for-penetration-testing-of-election-systems/

Gorman, B. (2023). Different types of hackers: white hat, black hat, gray hat, and more. *Different Types of Hackers: White Hat, Black Hat, Gray Hat, and More*. https://www.avg.com/en/signal/types-of-hackers

How ethical hackers are trying to protect the 2020 U.S. elections. (2023, 23 oktober). venturebeat. https://venturebeat.com/business/how-ethical-hackers-protect-2020-u-s-elections/

Schellevis, J. (2023, 12 september). Hacker ontdekt kwetsbaarheid in telsoftware verkiezingen: "Minder dan uur werk". *NOS*. https://nos.nl/artikel/2490218-hacker-ontdekt-kwetsbaarheid-in-telsoftware-verkiezingen-minder-dan-uur-werk

The Center for Election Innovation & Research. (2023, 10 February). *2022 Voter Registration Database Security Report | CEIR*. https://electioninnovation.org/research/2022-vrdb-security-report/

The Value of a Trusted Crowd of Ethical Hackers for Election Security. (2021, januari). Nass. https://www.nass.org/sites/default/files/2021-01/synack-white-paper-nass-winter21.pdf